

# User Manual

**Entegra™**

Version 2.0.1 for Microsoft® SQL Server™ 7.0 and 2000



This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Lumigent Technologies, Inc. Provides this document and the software described in this document "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Lumigent Technologies, Inc., except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Lumigent Technologies, Inc. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document may include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Lumigent Technologies, Inc. may make improvements in or changes to the software described in this document at any time.

**© 2002 - 2003 Lumigent Technologies, Inc., all rights reserved.**

U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the Government is subject to the terms of the Lumigent standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

Lumigent, Entegra, and the Lumigent logo are trademarks or registered trademarks of Lumigent Technologies, Inc. All other names and trademarks are property of their respective owners and are protected by the laws of the United States and other countries. Entegra uses technology that is the subject of one or more U.S. patent applications of Lumigent Technologies, Inc.

Sun, Sun Microsystems, the Sun Logo, Java, and Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft and SQL Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

This product includes software under license from Wireless Trading Ltd. and Sun Microsystems. Inc.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). See file "Apache Software License" or <http://www.apache.org/licenses/LICENSE> for more information.

---

# Contents

<b>About This Book .....</b>	<b>i</b>
Intended Audience .....	i
Other Information Available from Lumigent .....	i
Conventions.....	i
Contacting Lumigent Technologies.....	i
 <b>Chapter 1: Introduction .....</b>	 <b>1</b>
<b>How Entegra works.....</b>	<b>1</b>
<b>Why Entegra is better than other solutions .....</b>	<b>1</b>
<b>System Overview.....</b>	<b>2</b>
Architecture .....	3
Major Components .....	3
Major Functions.....	5
 <b>Chapter 2: Installing Entegra .....</b>	 <b>9</b>
<b>Before You Install.....</b>	<b>9</b>
Overview .....	9
Hardware/Software/Operating System Requirements .....	10
Network Requirements.....	11
Security Requirements .....	11
<b>Installing.....</b>	<b>14</b>
Prerequisites.....	14
Procedure .....	14
<b>Upgrading.....</b>	<b>17</b>
Upgrading the EMC.....	17
Upgrading the Web Server .....	22
Adding the SELECTs Feature to an Existing Entegra Environment .....	23
 <b>Chapter 3: Configuration .....</b>	 <b>23</b>
<b>Required Tasks.....</b>	<b>23</b>
<b>Optional tasks.....</b>	<b>23</b>
<b>Configuration Wizards Overview .....</b>	<b>23</b>
Add Audited Server Instance Wizard.....	23
Add Database Wizard .....	23
Add Repository Server Instance Wizard.....	23
Add Repository Wizard .....	23
Add/Remove Tables Wizard.....	23
Add/Remove Views Wizard.....	23
Add Collection Agent Wizard .....	23
Change Collection Agent Wizard.....	23
<b>Using the Configuration Wizards.....</b>	<b>23</b>
Overview of an Initial Entegra Installation.....	23

Adding a SQL Server Instance to Audit .....	23
Adding a Repository Server Instance .....	23
Adding a Repository.....	23
Adding a Database to Audit.....	23
Adding/Removing Tables.....	23
Selecting Audit Settings for Individual Tables.....	23
Selecting Audit Settings for Multiple Tables .....	23
Adding/Removing Columns .....	23
Selecting the Logical Key .....	23
Adding/Removing Views.....	23
Adding a Collection Agent.....	23
Changing a Collection Agent.....	23
<b>Using Multiple Entegra Management Consoles.....</b>	<b>23</b>
<b>Configuration Examples.....</b>	<b>23</b>
Example 1: Setting up two machines as an Entegra environment .....	23
Example 2: Setting up a distributed Entegra environment on three machines .....	23
Example 3: Variation of setting up three machines as an Entegra environment .....	23
Example 4: The SQL Server instance being audited is part of a cluster.....	23
 <b>Chapter 4: Archiving.....</b>	 <b>23</b>
<b>Archiving Process .....</b>	<b>23</b>
<b>Specifying Archive Options.....</b>	<b>23</b>
SQL Backup Log Handling.....	23
Entegra Intermediate File Handling.....	23
Purging Repository Audit Data.....	23
<b>About Restoring Audit Data.....</b>	<b>23</b>
Restoring Purged Audit Data.....	23
 <b>Chapter 5: Entegra Management Console Reference .....</b>	 <b>23</b>
<b>Navigation Tree.....</b>	<b>23</b>
Entegra Management Console_0.....	23
Audited Server Instances.....	23
Audit Data Repositories .....	23
Collection Agents .....	23
 <b>Chapter 6: Using the Entegra Browser .....</b>	 <b>23</b>
<b>Necessary Permissions .....</b>	<b>23</b>
<b>Starting the Entegra Web Server .....</b>	<b>23</b>
Shortcuts .....	23
<b>Logging On .....</b>	<b>23</b>
<b>Viewing the Repository with the Entegra Browser.....</b>	<b>23</b>
<b>Sorting and Filtering Data.....</b>	<b>23</b>
Showing/Hiding Columns .....	23
Filtering Data.....	23
Viewing Details .....	23

<b>Chapter 7: Troubleshooting .....</b>	<b>23</b>
Entegra Management Console Issues.....	23
<b>Web Server and Browser Issues.....</b>	<b>23</b>
Error Starting Web Server.....	23
<b>Event Log Errors .....</b>	<b>23</b>
 <b>Appendix A: Repository Schema.....</b>	 <b>23</b>
<b>Entity Relationship Diagram .....</b>	<b>23</b>
<b>Schema Tables.....</b>	<b>23</b>
lumtransactions_x.....	23
lumdetails_x.....	23
lumtracedetails_x .....	23
lumtables_x.....	23
lumkeydesc_x .....	23
lumkeys_x .....	23
lumservers_x.....	23
lumdatabases_x .....	23
lumsessions_x.....	23
lumphysicalattributes_x .....	23
lumhosts_x.....	23
lumdomains_x.....	23
lumapplications_x.....	23
lumlogins_x.....	23
lumosusers_x.....	23
lumopcodes_x .....	23
lumtranstable_x .....	23
lumowners_x .....	23
 <b>Appendix B: Restrictions.....</b>	 <b>23</b>
Component Setup Restrictions.....	23
Auditing Restrictions.....	23
Other Restrictions .....	23
 <b>Appendix C: Configuring the Entegra Web Server with IIS.....</b>	 <b>23</b>
Procedure .....	23
 <b>Index .....</b>	 <b>23</b>



---

# About This Book

This User Manual provides conceptual information about the Entegra product, as well as installation, configuration, and usage information. This book defines terminology and various related concepts.

## Intended Audience

This book provides information for database administrators and individuals responsible for installing, configuring, and using Entegra.

## Other Information Available from Lumigent

Lumigent provides the following information resources:

Resource	Information
<i>Quick Start Guide</i>	Provides overview information about Entegra, as well as planning, installation, and usage information. Also provides usage information for the Entegra Browser.
<i>Help</i>	Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.
<i>FAQ</i>	Provides answers to frequently asked questions; available from the Lumigent website, <a href="http://www.lumigent.com">www.lumigent.com</a> .

## Conventions

This book uses the following conventions to help you identify items throughout the documentation.

Convention	Used For...
<b>Bold</b>	<ul style="list-style-type: none"><li>Window and menu items</li><li>Technical terms, when introduced</li></ul>
<i>Italics</i>	<ul style="list-style-type: none"><li>Book and CD-ROM titles</li><li>Variable names and values</li><li>Emphasized words</li></ul>
Fixed Font	<ul style="list-style-type: none"><li>File and folder names</li><li>Commands and code examples</li><li>Text you must type</li><li>Text (output) displayed in the command-line interface</li></ul>

## Contacting Lumigent Technologies

Lumigent Technologies, Inc. is dedicated to safeguarding the integrity and availability of enterprise data. Please contact us with your questions and comments. We look forward to hearing from you.

To register your Entegra software, either register online at [www.lumigent.com](http://www.lumigent.com), or return the registration card enclosed in your product package. Benefits of registration include notification of product updates and upgrades.

For support around the world, please contact your local partner. If you cannot contact your partner, please contact our Technical Support team.

<b>Telephone:</b>	(1) (978) 206-3677
<b>Email (support):</b>	<a href="mailto:support@lumigent.com">support@lumigent.com</a>
<b>Email (sales):</b>	<a href="mailto:sales@lumigent.com">sales@lumigent.com</a>
<b>Web Site:</b>	<a href="http://www.lumigent.com/support">www.lumigent.com/support</a>

Subscribers to the Entegra software maintenance and support plan receive product updates and unlimited priority technical support via phone or email for twelve months. This support covers a variety of issues, including installation and configuration, use of product features, and consultative assistance on using Entegra. For more information, contact your sales representative.



---

# Chapter 1: Introduction

Entegra helps organizations address data privacy and security requirements with a complete audit of database activity. Entegra provides answers to the question “who is doing what to which data when?”

## How Entegra works

Entegra is designed to monitor, and optionally alert on, database activity, providing a complete record of access to data and database structure. Entegra provides an audit trail of data modifications and changes to database schema and permissions.

Entegra uses low-impact data agents that harvest information about database activity and optionally generate alerts on changes to database structure and permissions. A single console easily configures and controls these data agents across the enterprise to archive transaction information to common repositories. Lumigent’s proprietary technology minimizes performance impact by avoiding costly triggers. Entegra is designed to be easy to administer, with simple scheduling across multiple database platforms, and a common history repository.

## Why Entegra is better than other solutions

Lumigent’s approach is built on proven and proprietary technology for analyzing the database transaction log. Lumigent Entegra provides critical tracking of database activity without the performance overhead of triggers. There are three common alternative approaches to auditing data activity – these approaches miss certain kinds of activity, introduce a false sense of security, and interfere with runtime performance. The approaches are, as follows:

- changing the source code
- sharing a portal
- triggers

## Changing the Source Code

One approach involves changing the source code of every application that might be used to access data. Planning, implementing, and testing these changes are costly and time-consuming. Also, access outside of these applications (for example, via a database administrative console) is not captured, thus providing incomplete coverage.

## Sharing a Portal

Some application architectures funnel access to data through a shared portal; however, this technique works only for portal-enabled applications, requires software changes, and cannot capture access outside of those applications.

## Triggers

Traditional methods of capturing data access at the database server utilize database triggers. These triggers have the following disadvantages:

- cannot capture data-viewing activity
- cannot capture changes to database schema or permissions
- are often hard to write correctly
- add substantial performance overhead
- require minimizing the number of actions to record

Only Entegra captures changes to database structure and permissions, and no other approach offers Entegra's complete management, collection, and reporting capabilities.

# System Overview

This section provides an overview of the system architecture and describes the major components and functions of Entegra.

## Architecture

The following diagram illustrates the architecture of the Entegra system.



The entire Entegra system is configured and administered using the **Entegra Management Console**, a Microsoft Management Console snap-in.

Generally, Entegra works as follows:

1. Components, called **Collection Agents**, collect audit data from target Microsoft® SQL Server™ instances, and transmit the data in proprietary format to **Repositories**, where the data is stored.
2. An **Entegra Web Server** queries the data and serves it to a Web interface (the **Entegra Browser**) that can be accessed from any browser.
3. At predetermined intervals, audit data can be archived on disk and cleared from the Repository to make room for new data.

## Major Components

This section provides an overview of the following major components of Entegra:

- Audited Objects
- Data Collection Agents
- Repository
- Entegra Management Console
- Entegra Web Server and Browser

### Audited Objects

Audited objects include the following hierarchy of SQL Server objects:

- server instances (referred to in this book as **Audited Server Instances**)
- databases
- tables
- columns

By default, you specify a server instance and a database, then Entegra audits all tables and columns in that database; however, you can fine-tune this configuration to exclude tables and/or columns of your choosing.

## Data Collection Agents

Data Collection Agents can be installed on any Windows machine in the network. A Data Collection Agent may be assigned to one or many audited SQL Server instances. It is responsible for collecting audit data from the SQL transaction logs of the server instances and transmitting that data to the Repository. Because the Data Collection Agent need not be installed on the same machine that hosts an Audited Server Instance, performance impact is minimal even when auditing high-traffic databases.

A data definition language (DDL) Collection Agent resides on the same machine as a SQL Server and monitors DDL events on that server instance. When a DDL event is detected, the Collection Agent optionally records it in the Windows Event Log and/or sends an email message to the recipient of your choice.

A Repository Agent resides on the same machine as the Repository. This agent is responsible for receiving audit data from the Collection Agents and importing the audit data into the Repository.

Only the Data Collection Agent is exposed to your control. The other Agents operate invisibly and are managed by internal Entegra processes.

## Repository

A **Repository** is a set of SQL tables that stores all audited data, as well as metadata that enables the other Entegra functions. A single Repository may store audit data from multiple SQL Server instances and databases.

You may also license and set up additional Repositories to host audit data from different databases. Since the reporting and viewing of audit data are done on a per-Repository basis, all data that you want to view in a single report should be directed to the same Repository.

## Entegra Management Console

The Entegra Management Console, a Microsoft Management Console snap-in, is the tool you use to set up and configure your Entegra environment, and to monitor collection history. The Management Console automatically deploys Agents and other software components across the enterprise as necessary.

## Entegra Web Server and Browser

The Entegra Web Server and Browser allow you and others in your organization to view audited data in a familiar web browser. The Entegra Browser's powerful filtering capabilities make it easy to understand your data and find the information you need. You can also use the Entegra Browser to print reports with your data.

## Major Functions

This section provides an overview of the following major functions of Entegra:

- Configuring the Entegra Environment
- Collecting Audit Data
- Storing Data
- Archive Files
- Viewing and Managing the Data

## Configuring the Entegra Environment

The first major function necessary for auditing your data with Entegra is configuring your Entegra environment. Configuring enables Entegra to automatically perform its next two major functions: collecting audit data and storing the data. After which, you can view and manipulate the data.

The installation program provided with Entegra installs the Entegra Web Server and Entegra Management Console. You perform the remainder of the configuration tasks with the Entegra Management Console.

## Required tasks

To begin auditing, you need to accomplish the following tasks:

- Specify at least one SQL Server instance that you want to audit. Then, for each audited server, specify at least one database to audit.
- Specify at least one SQL server instance to be a Repository Server, and create at least one Repository to receive audit data.

## Optional tasks

You can also perform the following optional tasks with the Entegra Management Console:

- Set up alerts and notifications using email and/or the event log.
- Create multiple Repositories, on the same server or different servers, to receive audit data from multiple Audited Server Instances and/or databases. Note that one repository can hold data from multiple Audited Server Instances but you can only assign one repository to an Audited Server.
- Select what operations to audit for each table (SELECT, INSERT, UPDATE, DELETE).

- Fine tune the columns to audit in each table.
- Specify the columns that identify the unique row (using a logical key) in one or more audited tables.

All of the above tasks are described in more detail in Chapters 2 and 3.

## Collecting Audit Data

Data collection is performed by components, called **Collection Agents**, which run as Windows services. A single Collection Agent may be responsible for any number of databases on any number of Audited Server Instances. Typically, collection is performed on a fixed schedule that you set up. You can also manually initiate a collection task at any time.

When a Collection Agent launches – either in response to a manual command or as part of a scheduled task – it does the following:

1. The Collection Agent reads its configuration information from the Windows registry of the machine on which it is running. This registry information tells the Collection Agent which SQL server instance it is responsible for.
2. The Collection Agent then launches a collection process for each Audited Server Instance.
3. The information about each Audited Server Instance, including which database to audit and which table and column within that database to audit, is stored on the server machine. The Collection Agent reads this configuration information upon connecting to the Audited Server Instance.

Keeping this information on the audited server rather than on the Collection Agent's machine allows you to manage the Audited Server Instance from multiple locations, and ensures that your audit configuration is preserved in the event of a cluster failover or other problem.

The following types of data can be collected:

- data modification language (DML) operations
- data definition language (DDL) operations
- transaction information
- session information
- security events

In addition, data view (SELECT) queries can be collected, although this information is gathered differently than described above (see next section).

4. After the data is collected, it is packaged into **Intermediate Files** – one for each database.
5. The Collection Agent transmits these files to the Repository Agent (see next section).
6. The Collection Agent stores a complete record of its own processes in a history database on the Audited Server Instance machine. The Intermediate File is archived to allow for full recoverability. (For more details on the archiving feature, see Chapter 4.)

## Auditing SELECTs

Audit data about SELECT statements performed on Audited Server Instances is collected via SQL Server's trace function. All information generated by SQL Trace is stored on the machine that hosts the Audited Server Instance in a location that you specify. By default, the trace files are stored on the audited server machine in a subdirectory of the Program Files\Lumigent\Entegra\Data directory.

Periodically, the Entegra Collection Agent gathers this data, filters it, and appends it to Intermediate Files. It is then imported into the Repository along with all other audit data.

SELECTs is licensed separately from the auditing of DDL/DML activity. Contact Lumigent customer support for details.

## Logical Keys

Logical keys are used to determine what defines a unique row for any given SQL table. By selecting a particular column or set of columns as the logical key for a table, you enable Entegra to identify unique rows in the audited dataset, and to reconstruct this data in a useful way.

When you set up a table for auditing, Entegra selects columns to create a logical key for the table – typically by detecting the logical key, if one is already established for the table. If no logical key is selected, Entegra attempts to determine the most logical selections. After setup is complete, you can modify or fine-tune Entegra's selections manually for each table.

## Storing Data

Audit data is stored in a **Repository**, which is a set of SQL tables. (The complete schema of the Repository is available in Appendix A.) A single Repository may contain audit data from one or many SQL databases. The Repository may reside on the same machine (SQL instance) as a database being audited or on a separate machine/instance.

Importing data to a Repository is performed by a component called a **Repository Agent** that runs as a Windows service on the Repository machine. (Unlike the Collection Agent, which can be installed on a separate machine from the Audited Server Instance, the Repository Agent must reside on the same machine as the Repository.)

After an Intermediate File is received from the Collection Agent, the Repository Agent extracts the data from the Intermediate File and uses it to populate the Repository. This process is called **importing**. The data is now stored and ready to be viewed and queried. The Intermediate File is also stored on the Repository machine (or on a separate machine) as an archive (see Chapter 4).

## Archive Files

Collected audit data is stored in an archive file. This archive file is automatically imported into the repository.

Repositories may become quite large over time, so you may want to purge older audit data from the repository. A purge speeds up reporting and importing, but also makes the older audit data unavailable in the Entegra Browser UI.

To report on older data that has been purged out of the repository, Entegra creates a repository that contains only older data. This repository cannot be used for importing newer data as it may contain a discontinuous date range.

The Repository Agent is used to import the archive files for the date range desired into the report repository. You may then use the Entegra Browser UI to connect to the report repository and view the audit data for the desired date range. See Chapter 4 for more information.

## Viewing and Managing the Data

The three primary ways to view and manage the collected audit data are, as follows:

- Interactive reports
- Scheduled reports
- Custom reports

### Interactive reports

You can create and dynamically revise reports using the **Entegra Browser**. This graphical web-based application enables you to view, sort, and filter audit information, and produce reports.

Data for the Entegra Browser is provided by the **Entegra Web Server** component, which is installed by the Entegra setup program.

### Scheduled reports

After using the Entegra Browser to design a report, you can schedule it to run automatically at regular intervals using the Windows scheduler.

### Custom reports

You can interface directly with the data in the Repository, either by running queries through SQL Query Analyzer or using a third-party report creation application. Complete documentation of the Repository schema is available in the Appendix at the end of this manual. Further detail is provided in Chapter 6.



---

# Chapter 2: Installing Entegra

## Before You Install

Setting up Entegra on your system involves the installation of several software components that may reside on numerous machines.

To facilitate a smooth installation process, this chapter outlines the decisions you need to make and the hardware, software, and network components that you need before you install Entegra.

## Overview

You need to configure a set of server machines to run the various components of the Entegra system. The following conditions and restrictions apply:

- A Collection Agent may be installed on the same machine as the databases being audited or it may run on a separate machine.
- A Repository Agent is automatically installed on the same machine as the Repository for which it is responsible.
- The Management Console and Web Server may be installed on any machine that has sufficient connectivity to the other components' machines.
- Audit data can be viewed in an ordinary Web browser on any machine that has access to the Web Server machine.

All components – the Agents, Audited Server Instance, Repository, and Management Console – may reside on the same machine. However, for optimal performance, it is recommended that you place at least the Repository on a different machine from the audited server.

Note: If you are installing the Entegra product in a clustered environment, refer to the information in Appendix B Restrictions/Limitations. For an example of how to install in a clustered environment, see Chapter 3, example 4.

Entegra components require a server-class operating system such as Windows® 2000 or XP. The only exceptions are the client machine being used to browse the Repository (this machine may run any operating system capable of running the required Web browser; see below) and the machine hosting the Audited Server (Entegra supports Windows NT 4.0 with Service Pack 6 for this machine, in addition to Windows 2000 and XP).

For obvious reasons, all machines in the Entegra environment must be able to reach each other over a network connection, although they need not all be in the same Windows domain.

# Hardware/Software/Operating System Requirements

The following sections provide the requirements for each Entegra component. Depending on your desired configuration, the same machine may be described by two or more of the following sections. All required components are included with the Entegra setup program.

## Entegra Web Server

The Web Server only needs connectivity to the Repository Server and Repository databases.

The Web Server requires a server-class machine running at least 500 MHz processor speed with at least 512MB of RAM and 1GB of available disk space.

The Web Server requires the following software:

- Windows 2000, Windows 2003, Windows NT or Windows XP
- SQL Client components
- The most recent version of Microsoft's JDBC driver

The Entegra installation media provides a link to the JDBC download site.

## Audited Server Instance

Because the Audited Server Instance is already running SQL Server 7.0 or 2000, it generally meets the hardware and software requirements of Entegra (by virtue of meeting the requirements for SQL Server).

The SQL databases to be audited should be set to Full Recovery Mode. This mode setting is important because if this mode is not set, some audit data may be lost. Backups also need to be performed on a regular schedule.

Supported platforms include Windows 2000, Windows 2003, Windows NT 4.0 with Service Pack 6, and Windows XP.

## Repository Server/Repository Agent

The Repository Server should be a server-class machine with at least 1GHz processor speed, 512MB of RAM, and 20GB of available disk space. These minimums are typical; the exact hardware requirements vary greatly depending on the number and size of databases being audited and the amount of audit data (number of transactions).

The following formula may be useful in determining the disk space necessary for collections:

Transaction log size of 100MB x 3 x 10days = 3GB.

The Repository Server must be running SQL Server 2000 and it must support SQL authentication login (vs. Windows-only).

SQL 7.0 is not supported for the Repository.

SQL Service Packs 2 and 3 are fully supported.

Supported platforms include Windows 2000, Windows 2003, Windows NT 4.0 with Service Pack 6, and Windows XP.

## Collection Agent

If the Collection Agent runs on a separate machine that is not also an Audited Server Instance, it requires a minimum of 512MB of RAM and must have SQL Client components installed.

Supported platforms include Windows 2000, Windows 2003, Windows NT 4.0 with Service Pack 6, and Windows XP.

## Entegra Management Console

The Entegra Management Console can run on any server-class machine capable of running the Microsoft Management Console.

SQL Server client components must be installed on the Management Console machine.

Supported platforms include Windows 2000, Windows 2003, and Windows XP.

The Entegra Management Console cannot run on Windows NT 4.0 or earlier.

## Entegra Browser

The Entegra Browser requires Microsoft Internet Explorer 6.0 or later. Users can access the Entegra Browser from any machine capable of running this application.

## Network Requirements

The various machines running Entegra need not be on the same domain, but they must have network connectivity to each other.

The agent machines must be running the Remote Registry Service.

## Security Requirements

To allow you to meet your corporate security needs, the security requirements for installation, configuration, and ongoing operation of Entegra are designed for maximum flexibility, and therefore are fairly complex.

It is recommended that you create a Windows user on your domain to be used only by Entegra. This login, referred to in this book as "EntegraLoginUser," is used by the Entegra Management Console and the following Agents to perform various tasks:

- Collection Agent Account
- Repository Agent Account
- Account currently running on the machine hosting the Console

The permissions required by this login are described below.

Note: Although the following information is broken down by Entegra component, you may install multiple components on the same physical machine; therefore the same machine may be described by more than one of the following sections.

The following sections are based on the use of Windows authentication to access all relevant SQL Server databases, as follows:

- databases being audited
- databases containing Repositories
- databases containing Entegra configuration information

You must enable EntegraLoginUser to access the necessary databases.

If you prefer to use SQL authentication for any of these databases, you can create a SQL login (for example, "EntegraSQLUser") to be used only by Entegra.

## Audited SQL Server Instance Service Privileges

The service login of each audited SQL Server instance must have sysadmin privileges in that audited server instance.

Because LMServer runs within SQL Server itself, and it uses Windows Authentication to log on to SQL Server, it must run as an account with sysadmin privileges in SQL Server, or Entegra can't collect session data, DDL, SELECTS, and alerts.

To determine whether the account has sysadmin access, do the following:

1. Log on to Windows using that domain account; then use Query Analyzer to connect to SQL Server.
2. Use Windows Authentication to connect, and then issue the following query:

```
SELECT SYSTEM_USER, IS_SRVROLEMEMBER('sysadmin')
```

The query returns two columns: the account name in the first column and the number 1 in the second column. If 0 is shown in the second column, then this account does not have sysadmin access and Entegra won't work.

## Audited Server Machine

On each machine hosting an Audited Server Instance, the Entegra login needs the following permission set:

- Read and Write access to the Windows Registry
- Read and Write access to the file system
- Read access to the directory where SQL Server backup files are stored
- System Administrator permissions on the SQL Server instance being audited (unless you plan to use SQL Authentication; see above). These permissions are used by the Collection Agent.

If you choose to implement the SELECTs auditing feature (see Chapter 1), the Entegra login also needs full access to the directory where you wish to store SQL trace files. For details, see Chapter 3.

## Repository Machine

On each machine hosting a SQL Server Instance that contains a Repository, the Entegra login needs the following permission set:

- Read and Write access to the Windows Registry
- Read and Write access to the file system
- Read access to the directory where SQL Server backup files are stored
- "Log On as Service" privileges (for the Repository Agent)
- System Administrator permissions on the Repository Server Instance, including the authority to create tables in the lumigent database (see Repository section below). (Does not apply if you plan to use SQL Authentication; see above.) These permissions are used by the Repository Agent.

By default, Repositories are created within the lumigent database. However, because users browsing the Repository with the Entegra Browser require a fairly high level of access permissions on the Repository database, you can install your Repository on a database other than lumigent for security purposes. (The Management Console's Add Repository Wizard provides a mechanism for doing this.)

For details on the permissions that are needed to log on to the Entegra Browser, see Chapter 6.

## Repository

While Entegra needs full permissions to read and write the Repository, you can create one or more read-only database accounts for Entegra Browser users that are viewing the audit data.

The only accounts that should have write access to the Repository tables in the Repository database are the Repository Agent and the Entegra administrator.

## Collection Agent Machine

On each machine hosting a Collection Agent (which may be separate from the machine hosting the Audited Server Instance), the Entegra login needs "Log On as Service" privileges. It must also have (at minimum) read access to all directories containing SQL transaction log backups for audited databases.

# Installing

This section provides you with the prerequisites and the instructions for installing Entegra. If you are upgrading Entegra, see the *Upgrading* section of this manual.

## Prerequisites

Before attempting to install Entegra, ensure the following:

- You have met the system requirements as provided in this chapter.
- The Entegra Management Console is not running.
- The Entegra Web Server service is stopped.

## Procedure

To install Entegra, do the following:

1. Run *setup.exe* from the Entegra version 2.0.1 media provided.

The “Installation” screen is displayed.



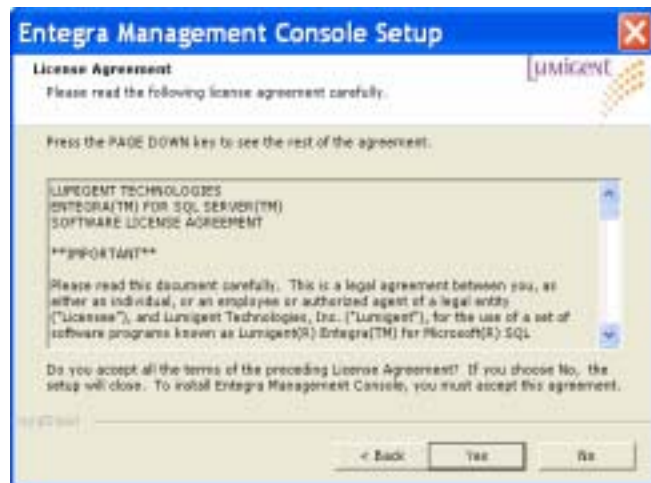
2. Click **Install Entegra Management Console**.

The Lumigent splash screen is displayed.



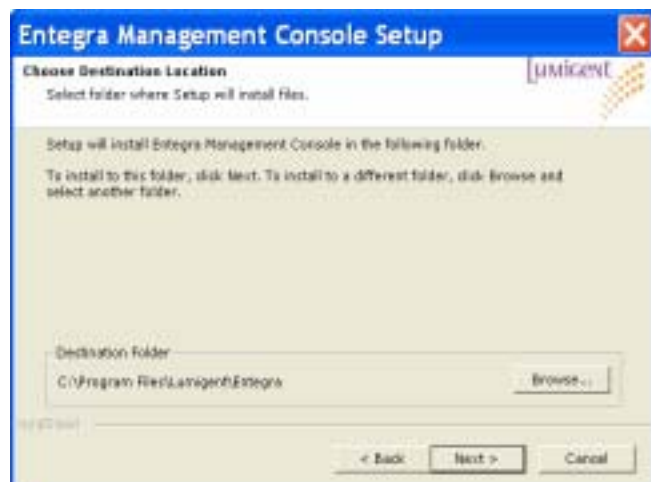
3. Click **Next**.

The "License Agreement" screen is displayed.

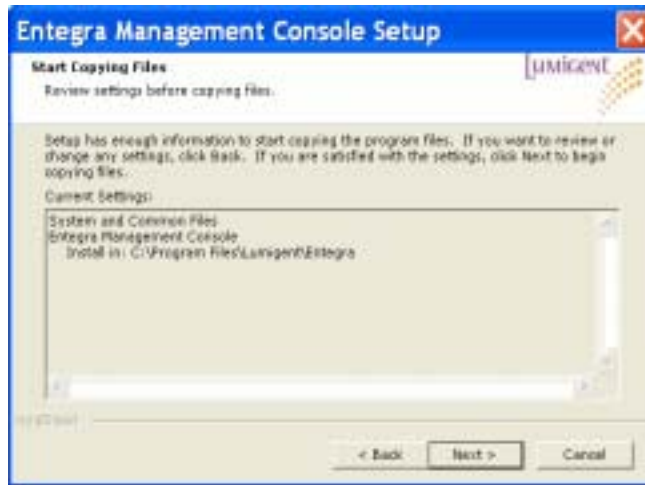


4. Read the licensing agreement, and then click **Yes**.

The "Choose Destination Location" screen is displayed.



5. Click **Browse** to choose a different location than the default, and/or click **Next**.  
The “Start Copying Files” screen is displayed.



6. Verify your destination location and then click **Next**.  
The “InstallShield Wizard Complete” screen is displayed.



7. To start the Entegra Management Console now and display the documentation, click **Finish**.  
The Entegra Management Console is displayed.



# Upgrading

You can upgrade to v2.0.1 from version 1.3 or later. If you have versions prior to v1.3, you must upgrade to v1.3 before you can upgrade to v2.0 or later.

## **CAUTION!**

The Entegra component upgrade process is irreversible.

To prevent loss of data, do the following:

1. Back up the configuration databases for each Audited Server Instance.
2. Back up the configuration databases for each Repository Server Instance.
3. Back up each database that hosts an Entegra Repository.

If you are upgrading all your repositories to version 2.0.1, you must do the following:

After you have upgraded the EMC, ensure that you right-click the **Entegra Management Console\_0** node and select **Upgrade** before you attempt to view any existing repositories.

## Upgrading the EMC

### **Prerequisites**

Before attempting to upgrade Entegra, ensure the following:

- You must have Entegra v1.3 or v2.0 installed to upgrade to v2.0.1.
- You meet the system requirements as provided in this chapter.
- The Entegra Management Console is not running.
- The Entegra Web Server service is stopped.
- You have backed up the files listed in the Upgrading section.

### **Procedure**

Be sure to perform this procedure on each machine running an instance of the EMC.

To upgrade the EMC to Entegra 2.0.1, do the following:

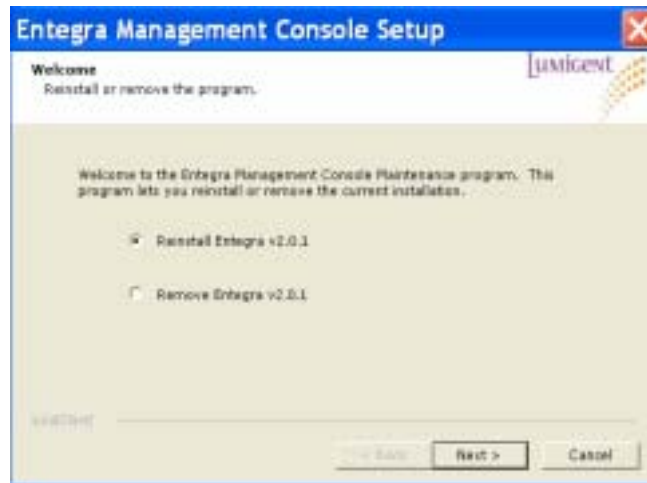
1. Close the existing Entegra Management Console and stop the Web Server service.
2. Run *setup.exe* from the Entegra 2.0.1 media provided.

The “Installation” screen is displayed.



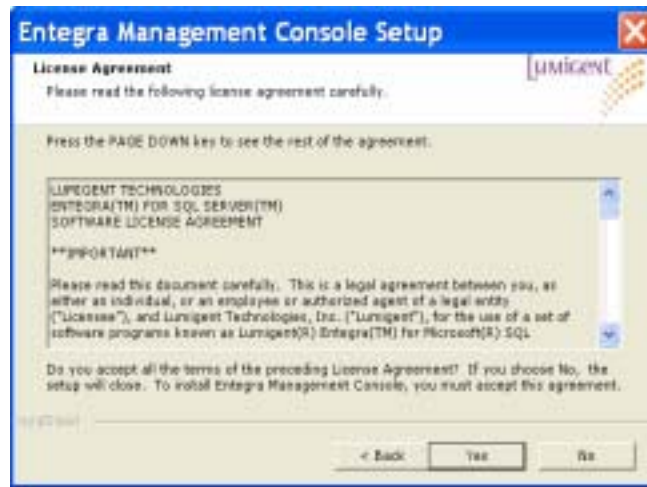
3. Click **Install Entegra Management Console**.

A Reinstall or Remove Entegra screen similar to the following is displayed.



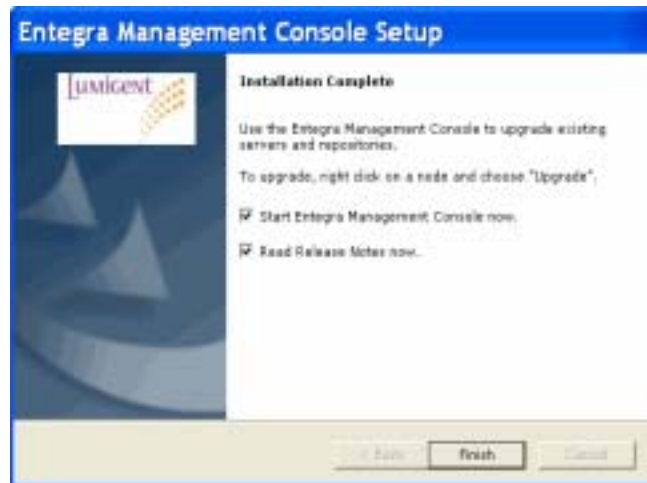
4. Click **Next**.

The “License Agreement” screen is displayed.



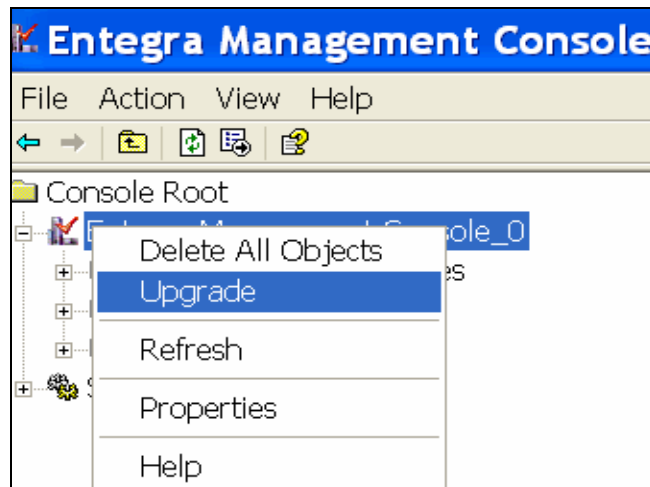
5. Read the licensing agreement, and then click **Yes**.

The “Installation Complete” screen is displayed.



6. Accept the default, **Start Entegra Management Console now**, and then click **Finish**.

The Entegra Management Console displays your configuration information as it was before you upgraded the EMC.



**CAUTION!**

The Entegra component upgrade process is irreversible.

7. To prevent loss of data, do the following:
  - a. Back up the configuration databases for each Audited Server Instance.
  - b. Back up the configuration databases for each Repository Server Instance.
  - c. Back up each database that hosts an Entegra Repository.
8. Right-click the top-level **Entegra Management Console\_0** node and select **Upgrade**.

The “Welcome to the Upgrade Wizard” screen is displayed.



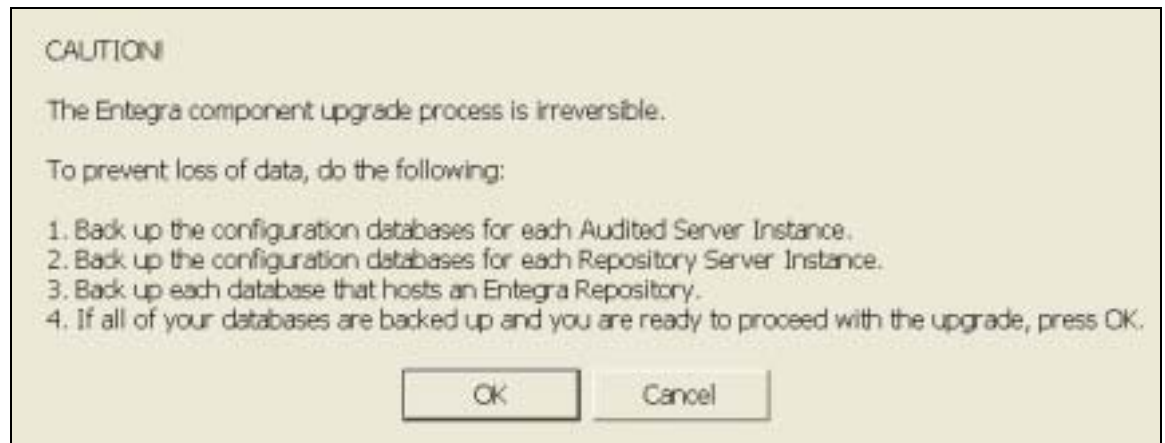
9. Click **Next**.

The screen that displays upgrade status is displayed.



10. Click **Finish**.

The following Caution screen is displayed.



11. Ensure you obey the Caution, and then click **OK**.

All Audited Server Instances, Collection Agents, Repository Server Instances, Repositories, and Repository Agents in your configuration are automatically upgraded. Collections proceed as normal.

**Important:** The amount of time required to upgrade increases according to the size of the repositories being upgraded.

## Upgrading the Web Server

To upgrade the Web Server to Entegra version 2.0.1, do the following:

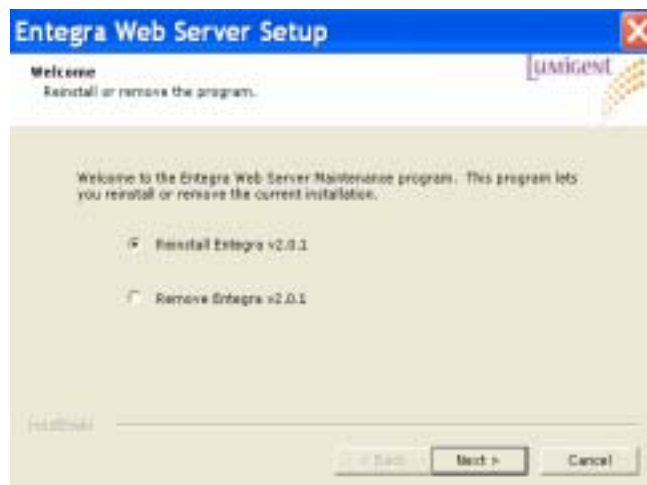
1. Run *setup.exe* from the Entegra version 2.0.1 media provided.

The “Installation” screen is displayed.



2. Click **Install Entegra Web Server**.

An Upgrade or Remove Entegra screen similar to the following is displayed.



3. Click **Next**.

The “License Agreement” screen is displayed.



4. Read the licensing agreement, and then click **Yes**.

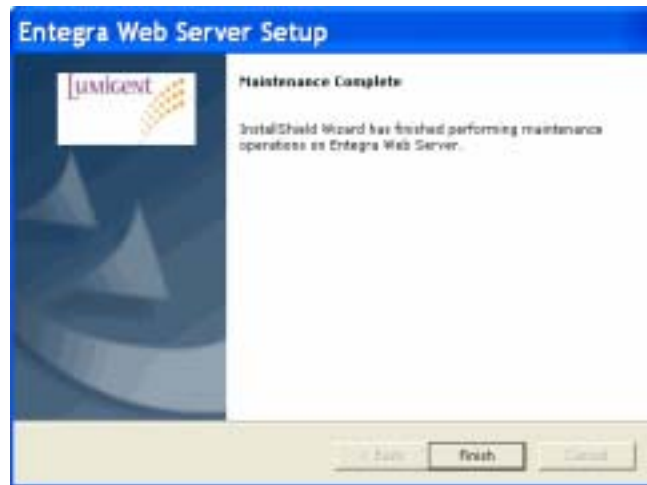
Note: If you are currently running the Web Server, a stop notice is displayed.

The “Microsoft JDBC Drivers Install Path” screen is displayed.



5. Confirm the location of the Microsoft JDBC drivers and then, click **Next**.

A “Web Server service is starting” notice is displayed, and then the “Maintenance Complete” screen is displayed.



6. Click **Finish**.



## Adding the SELECTs Feature to an Existing Entegra Environment

You can audit data about SELECT statements performed on Audited Server Instances. This data is collected via SQL Server's trace function. All information generated by SQL Trace is stored on the machine that hosts the Audited Server Instance, in a location that you specify.

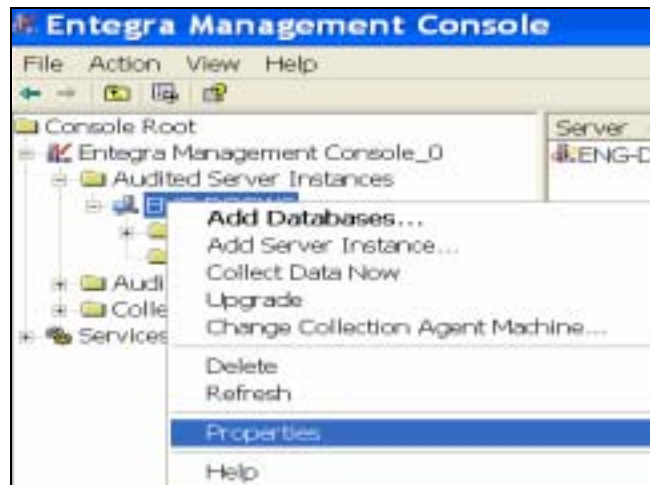
### Prerequisites

To add the SELECTs feature, you need an appropriate license key to enter during the procedure.

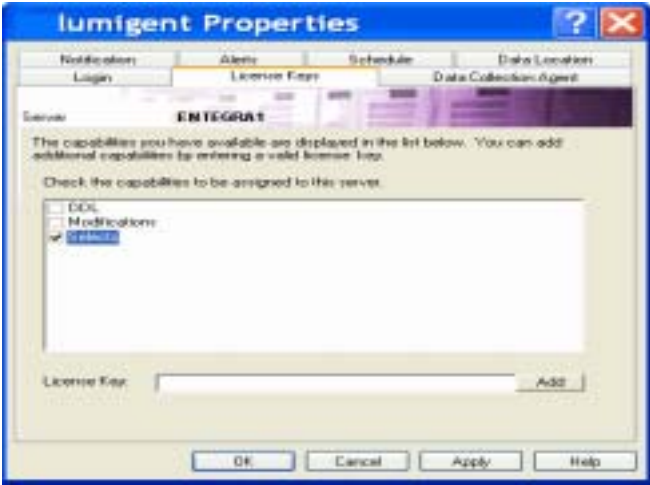
### Procedure

Be sure to perform this procedure on each machine running an instance of the EMC.

1. At the EMC, right-click the audited server instance, and then select **Properties**.



The screen that allows you to select your license capabilities is displayed.



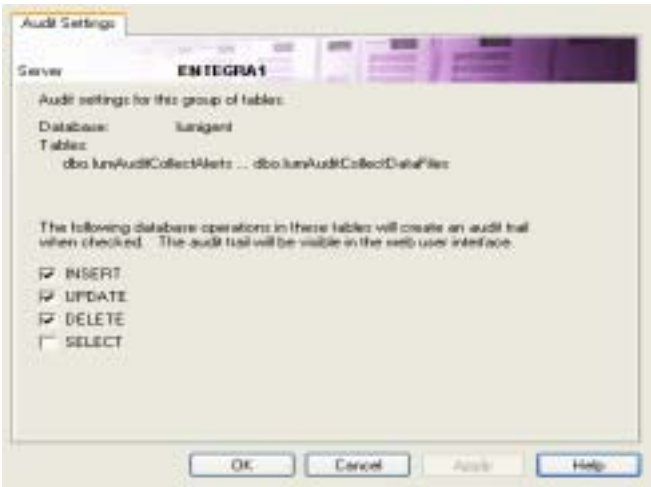
- 2. Click the **License Keys** tab, and then at the **License Key** text box, type or paste your SELECTs license key, click **Add**, select the **Selects** check box, and then click **OK**.
- 3. At the EMC, select the audited database node.

The audited tables are displayed in the right pane.

Table Name	Audit Type	Columns being audited
dbo.lumAuditCollectAlerts	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectConfigVars	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectDatabases	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectDataFiles	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectEventData	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectHistory	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectNotification	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectTables	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectTraceFiles	INSERT;UPDATE;DELETE	*

- 4. Are you selecting more than one table for audit?  
If yes, use **Shift+click** or **Ctrl+click** to select more than one table, right-click the selections, and then select **Properties**.  
If no, right-click the table, select **Properties**, and then click the **Audit Settings** tab.

The audit settings screen similar to the one below is displayed.



- 5. Select the **SELECT** check box and then click **OK**.
- 6. To verify that the tables are enabled for **SELECT**, ensure that **SELECT** is displayed in the **Audit Type** column, as shown below.

Table Name	Audit Type
dbo.lumAuditCollectAlerts	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectConfigVars	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectDatabases	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectDataFiles	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectEventData	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectHistory	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectNotification	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectTables	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditCollectTraceFiles	INSERT;UPDATE;DELETE;SELECT
dbo.lumAuditRepRepositories	INSERT;UPDATE;DELETE;SELECT
dbo.sysconstraints	SELECT
dbo.syssegments	SELECT



---

# Chapter 3: Configuration

Chapter 3 provides the necessary configuration options to begin auditing your data.

Now that you have successfully installed Entegra, you need to set up the necessary configuration options to begin auditing your data. The configuration tasks discussed in this chapter are performed by the Entegra Management Console (EMC).

The EMC is a Microsoft Management Console (MMC) snap-in that allows you to setup and configure your Entegra environment, including:

- defining objects (such as databases, tables, and columns) that you wish to audit.
- creating Repository Servers and Repositories to contain audit data.
- creating alerts for particular database activity types and assigning notification methods to these alerts.

## Required Tasks

To begin auditing, you need to accomplish the following tasks:

- Specify at least one SQL Server instance that you want to audit. Then, for each audited server, specify at least one database to audit.
- Specify at least one SQL server instance to be a Repository Server, and create at least one Repository to receive audit data.

## Optional tasks

You can also perform the following optional tasks with the Entegra Management Console:

- Set up alerts and notifications using email and/or the event log.
- Create multiple Repositories, on the same server or different servers, to receive audit data from multiple Audited Server Instances and/or databases.
- Select what operations to audit for each table (SELECT, INSERT, UPDATE, DELETE).
- Fine tune the columns to audit in each table
- Specify the columns that identify the unique row (using a logical key) in one or more audited tables.

Note: The unique row enables better detail in audit reports. Entegra does this automatically, but you may want to fine tune the logical key to add or remove the activity details that are included in the audit report / browser view.

The amount of data collected depends on the various types of activity in your database. If you have a large number of transactions, you may generate a lot of audit data. This means that you need to ensure adequate room for your repository's database, or you may want to reduce the following from being audited:

- types of transactions
- number of tables
- number of columns

A large number of transactions being audited increases the amount of time required to import the data into the Repository. When auditing a database for the first time, Entegra reads in all transactions available in all of the backup logs for that database. If there is a large amount of data in these logs, the first collection and import takes a significant amount of time.

The examples in the next sections demonstrate how to accomplish each of these tasks.

## Configuration Wizards Overview

The Entegra Management Console provides several wizards that facilitate the configuration process. The following sections provide an overview of the wizards. Examples of how to use these wizards to set up a complete Entegra environment are provided later in this chapter.

### Add Audited Server Instance Wizard

The Audited Server Instance Wizard sets up a specified SQL Server instance for auditing. You can also use this wizard to connect the Entegra Management Console to a previously-established Audited Server Instance (for example, if you have installed the Management Console on a new machine and wish to use it to administer your existing Entegra setup).

During the Audited Server Instance Wizard, you specify the following:

- server instance
- various login information
- auditing options
- whether to install the Data Collection Agent on the same machine that hosts the server instance or on a separate machine

Note that completing the Audited Server Instance wizard is not sufficient for Entegra to begin auditing. You must complete the Add Database Wizard for auditing to begin.

## Add Database Wizard

The Add Database to Audit Wizard sets up a specified database for auditing. The Add Database wizard can only be performed on a previously-established Audited Server Instance. To successfully use the Wizard, you must complete the Audited Server Instance wizard.

You can use the Add Database Wizard to add multiple databases simultaneously, provided that they are all on the same server instance.

The Add Database Wizard requires you to assign the new audited database to a Repository. If you have already created a Repository Server Instance and created a Repository, you can select the existing Repository during the Add Database Wizard. If no Repository exists yet, or if you wish to create a new Repository for this database, the Add Repository Wizard is incorporated into the Add Database Wizard.

During the Add Database Wizard, you may select the following optional features:

- Enable Data Modification auditing on all tables
- Enable SELECTs auditing on all tables and views

### Enable Data Modification auditing on all tables

You can set Entegra to audit all tables in the selected database (this is the default), or not. If you clear the **Enable Data Modification auditing on all tables** check box in the Add Database Wizard, you must complete the Add Table Wizard before auditing can begin.

The **Enable Data Modification auditing on all tables** check box is unavailable if there are no DML or DDL licenses assigned to the server.

### Enable SELECTs auditing on all tables and views

You can audit data about SELECT statements performed on Audited Server Instances. This data is collected via SQL Server's trace function. All information generated by SQL Trace is stored on the machine that hosts the Audited Server Instance, in a location that you specify. SELECTs keeps track of every SELECT statement issued against the tables being audited. The tables that are audited for SELECT have the SELECT opcode filter set.

SELECTs data is temporarily stored on the audited server and may take up a lot of disk space if there is a lot of activity on the tables and views being audited. Be sure to specify a SELECTs data directory with a lot of available disk space to avoid losing any audit information. The default disk space allocated is 500 MB.

The location of the SELECTs data directory can be set in the Audited Server properties on the **Data Location** tab.

The **SELECTs** check box is unavailable if there is no SELECT license assigned to the server. The SELECTs check box is also not available on SQL Server 7 servers.

## Add Repository Server Instance Wizard

The Add Repository Server Instance Wizard is generally used to re-establish an existing repository server configuration, or as a precursor to creating a Repository. This wizard is automatically incorporated into the Add Repository wizard when the Add Repository wizard is invoked from the Audited Repositories folder.

You specify the following information in this wizard:

- the Server instance (SQL 2000 or better) and login
- the Agent login (Windows or local system admin)
- Archive location
- Alerts notification

The Add Repository wizard uses the existing repository server if the Add Repository wizard is launched from the context menu of a Repository Server node.

This wizard is also incorporated into the Add Database wizard when that wizard is used to create a new repository.

You can also use this wizard to connect the Entegra Management Console to a previously-established Repository (for example, if you have installed the Management Console on a new machine and wish to use it to administer your existing Entegra setup).

## Add Repository Wizard

The Add Repository Wizard creates a new Repository to hold audit data. You must have a Repository Server Instance set up to host the Repository. If no Repository Server Instance exists when you begin the Add Repository Wizard, the Add Repository Server Instance Wizard is incorporated into the Add Repository Wizard.

During the Add Repository Wizard, you specify the following:

- the Repository Server Instance that hosts the new Repository
- the Repository name
- the database that contains the Repository

Note: Since the Repository is a set of SQL tables, it can reside in any database on the Repository Server Instance. By default, it is installed in the lumigent database.

Restriction: Using a non-alphanumeric character as the first character of a repository name can cause problems. It is recommended that you use an alphanumeric character to begin a repository name. You may use special characters (the following are accepted: @ \_ \$ #) elsewhere in the repository name.

When you use the Add Repository Server to connect to an existing Repository Server configuration, the EMC automatically picks up any Repositories that are established in that server instance.

## Add/Remove Tables Wizard

The Add/Remove Tables Wizard allows you to specify which tables in an audited database should be audited. If you cleared the **Enable Data Modification auditing on all tables** check box in the Add Database Wizard, you must run the Add Tables Wizard to specify at least one table to begin auditing.

It is not recommended changing settings during a collection or import. EMC returns an error message if it is not a good time to change the settings.



A logical key needs to be defined for any table on which you want to view activity details. The audited columns in the table are the columns that are displayed in the Activity Details pane on the web browser. You need to define both logical keys and audited columns to see any activity details for a transaction on that table.

## **Add/Remove Views Wizard**

The Add/Remove Views wizard is available on the Audited Database menu when the Audited Server Instance is SQL Server 2000 or better and has a SELECTs license assigned to it. A View is a way to select and view data from multiple tables at the same time. View transactions show up in the Audited Data browser as both a SELECT on the View and as a SELECT on each table associated with the View. This allows you to filter by View name or by table name and get a complete listing of SELECT transactions for each.

## **Add Collection Agent Wizard**

The Add Collection Agent Wizard is generally used to re-establish a connection to an existing collection agent. The Add Collection Agent wizard is automatically incorporated into the Add Audited Server Instance Wizard and the Change Collection Agent wizard if you specify an Agent machine that does not have an established collection agent.

## **Change Collection Agent Wizard**

The Change Collection Agent Wizard allows you to move a particular Audited Server's collection processing load to a different machine. You can reassign the Audited Server to an existing Agent that is already handling other Audited Servers.

If you specify an Agent machine that does not have an established collection agent, the Add Collection Agent Wizard is automatically incorporated into the Change Collection Agent wizard.

This is not a wizard that is generally run as part of initial configuration. You may want to change a collection agent if Entegra collections are negatively affecting performance on a production machine and you want to move this workload to a different machine. In this case the Change Collection Agent wizard smoothly transfers the workload from the old machine to the new machine. It is best to do this when no collections are taking place.

## **Using the Configuration Wizards**

This section provides step-by-step instructions on how to use the configuration wizards to set up your Entegra environment. Instructions are included for the following wizards:

- Adding a SQL Server instance to audit
- Adding a Repository Server Instance
- Adding a Repository
- Adding a Database to audit
- Adding/Removing Tables

- Selecting Audit Settings for Individual Tables
- Selecting Audit Settings for Multiple Tables
- Adding/Removing Columns
- Selecting the Logical Key
- Adding/Removing Views
- Adding a Collection Agent
- Changing a Collection Agent

## Overview of an Initial Entegra Installation

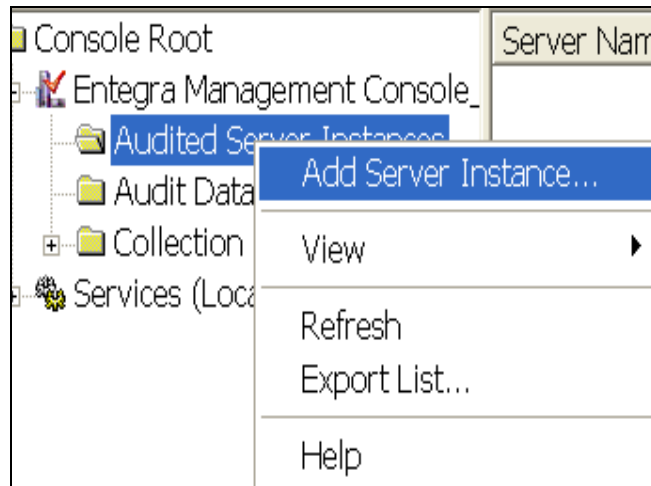
Installing Entegra for the first time requires you do the following:

1. Add a SQL server instance to audit
2. Add a database to audit.
3. Manually collect data.

## Adding a SQL Server Instance to Audit

To add at least one SQL server instance to audit, do the following:

1. At the EMC, right-click **Audited Server Instances**, and then select **Add Server Instance**.



The "Add Server Instance to Audit" screen is displayed.




2. Click **Next**.

The "Choose a database server to audit" screen is displayed.



For this screen, you need to consider the following:

If you want the Audited Server and the Collection Agent...	Then...
on the same machine	you can use the database login for the server and local service login for the agent or, you can use Windows login for both the audited server and the agent.
each on a different machine	it is highly recommended that you use Windows login for the audited server and the agent.  Note: The Windows account used to log on to the Audited Server is specified on the Agent logon page.

3. In the Database Server text box, type the database server you want to audit, or click the browse button  to display the available database servers as shown below. Select a database server, and then click **OK**.



4. If you want to connect using SQL Server authentication, click the **SQL Server authentication** radio button, and then enter a Logon Name and password.
5. If you accept the default **Collection Agent runs on the same machine as this database server**, click **Next**, and then go to step 7.

Or,

Clear the **Collection Agent runs on the same machine as this database server** check box, and then click **Next**.

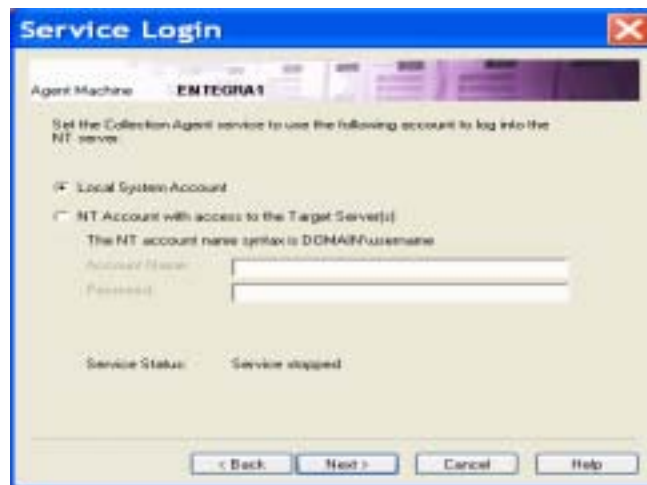
The screen that allows you to add a machine for the collection agent is displayed.



6. In the **Agent Machine** text box, type name of the machine from which you want to run the Collection Agent Service, and then click **Next**.

The "Service Login" screen is displayed.

Note: If the fields are not available and the Service Status indicates that the service is running, you can use MMC Services to manage the account.



7. Specify the login information that the Collection Agent uses to run its service, and then click **Next**.

The local system account is the default. Alternatively, you can specify a username and password. This account must have "logon as service" permission.

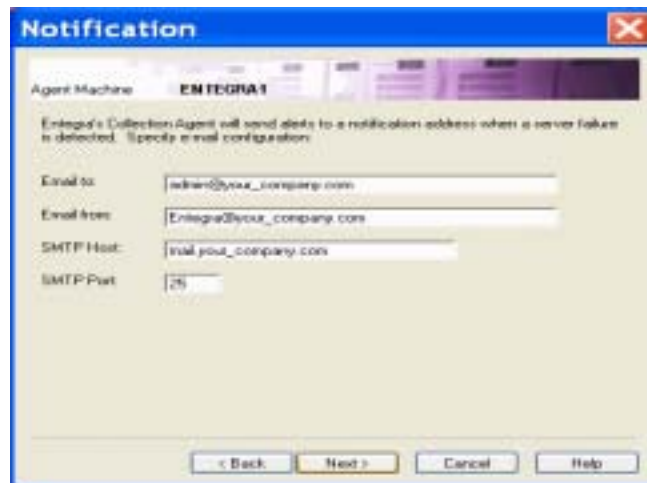
The “Data Collection Agent” screen is displayed.

Note: If the Installation Directory location box is not available, then there is already an Entegra component installed on that machine. Entegra installs all of its components to the same directory on a given machine.



8. Select the locations where you want the Collection Agent installed and where you want it to store its audit data files, and then click **Next**.

The “Notification” screen is displayed.



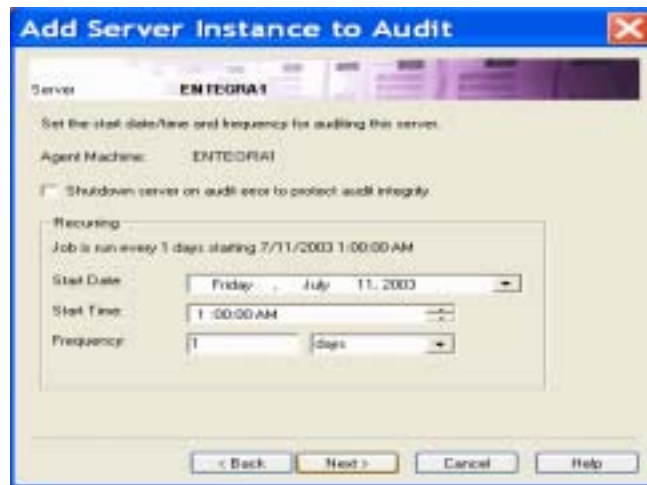
9. Enter email information for the Collection Agent to use when emailing you about collection failures. You must enter a To and From email address, and the name of your mail server, and then click **Next**.

The screen that allows you to select your license capabilities is displayed.



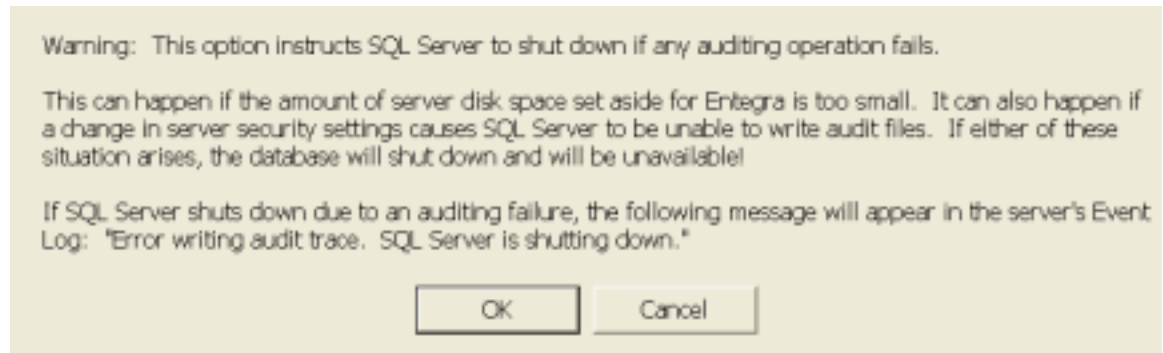
10. Type or paste the license key into the **License Key** text box and click **Add**.  
All features available in this key are displayed in the window.
11. Check the boxes next to the features that you wish to enable for this audited server instance, and then click **Next**.

The screen that allows you to set auditing frequency is displayed.



12. To choose the option, **Shutdown the server on audit error to protect audit integrity**, select the check box.

Note: If you select this option, the following warning is displayed:



13. Is this the first collection being performed?

If yes, do the first collection manually by setting the Start Date a day or two in the future, and then click **Next**.

Note: The first collection may take several hours if there are a large number of transactions in the database backup logs. You can access the Audited Server instance properties after the first collection is complete to fine tune recurring collections.

Recommendation: If there are automated backups, perform collections soon after the backup completes. For best performance, avoid overlapping backup and audit data collection operations.

If no, click the down arrows to select the start date, start time, and frequency for auditing the server, and then click **Next**.

The screen that allows you to specify how alerts are sent from the server is displayed.



14. Accept the default to **Add alert events to the event log on the server**, or clear the check box.

Recommendation: The event log always contains an accurate trail of DDL alerts, so it is recommended that you select the **Add alert events to the event log on the server** check box. If there are a large number of e-mail alerts (more than 100 per second) the e-mail alerts throttle back. If neither box is checked, you are not notified of DDL alert events and the following screen is not displayed.



15. To have alert events emailed, select the **Email to:** check box, make any modifications in the text boxes, and then click **Next**.

The screen that allows you to select alert events is displayed.



16. Select or clear the desired alert events check boxes, and then click **Next**.

Recommendation: It is recommended that you do not select the **Successful login** check box because of the large number of alerts generated by this audit. If these alerts are emailed to you, server performance may be impacted.

The screen that allows you to complete the configuration wizard is displayed.



17. Click **Finish**.

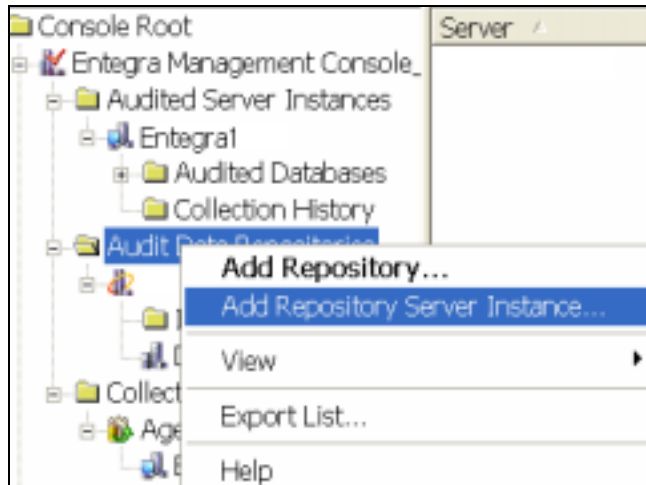
The Entegra Management Console automatically deploys the necessary software components to the Audited Server Instance. The EMC also deploys Collection Agents as needed.

Note: For each audited server, you need to specify at least one database to audit.

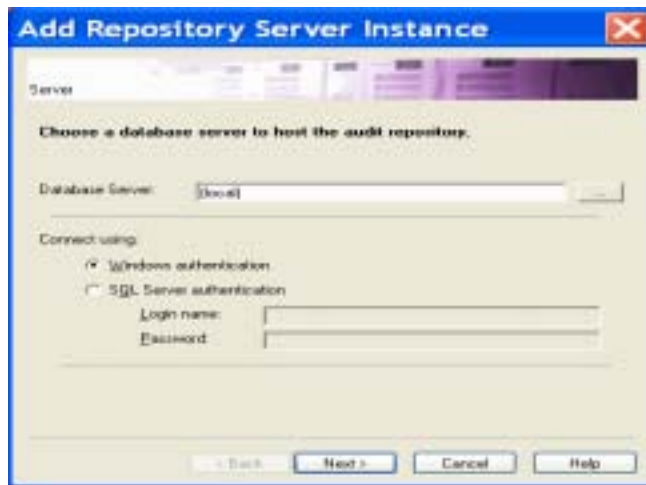
## Adding a Repository Server Instance

To add a Repository Server Instance, do the following:

1. At the EMC, right-click **Audit Data Repositories**, and then click **Add Repository Server Instance**.

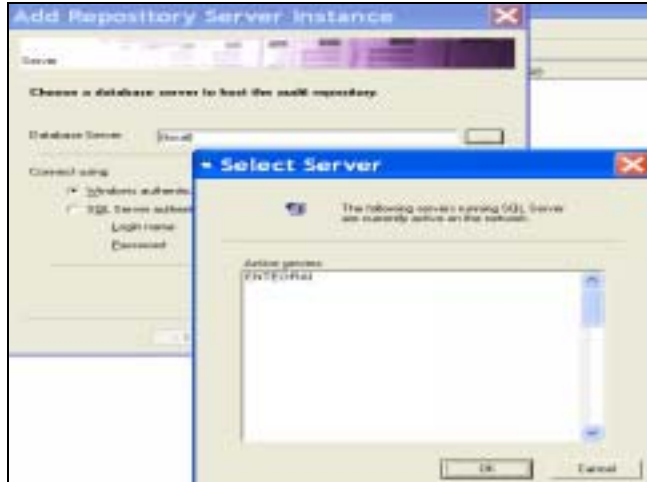


The “Add Repository Server Instance” wizard is displayed.



2. In the **Database Server** text box, type the database server you want to host your repository on, or click the browse button ... to display the available database servers as shown below. Select from the available database servers, and then click **OK**.

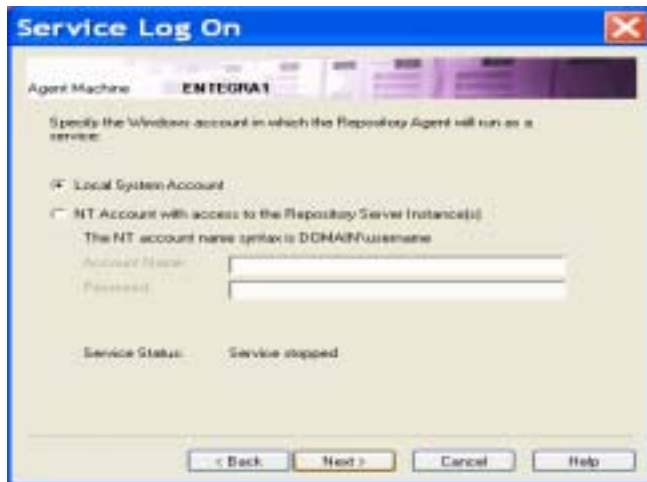
Note: Only SQL 2000 Servers may be selected. Selecting a SQL 7 Server generates an error message.



3. If you want to connect using SQL Server authentication, click the **SQL Server authentication** radio button, enter a logon name and password, and then click **Next**.

Note: If there is already a repository established on this machine, go to step 7.

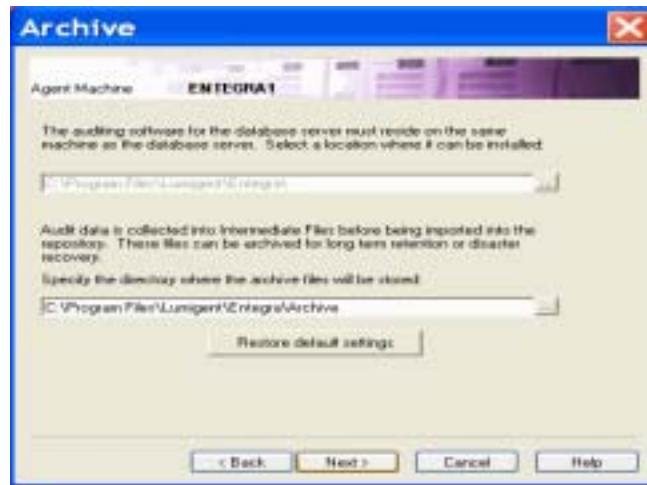
The "Service Log On" screen of the Repository Agent Wizard is displayed.



4. Click **Next** to accept the **Local System Account** default, or click **NT Account with access to the Repository Server Instance(s)** radio button and type the Account Name and Password, and then click **Next**.

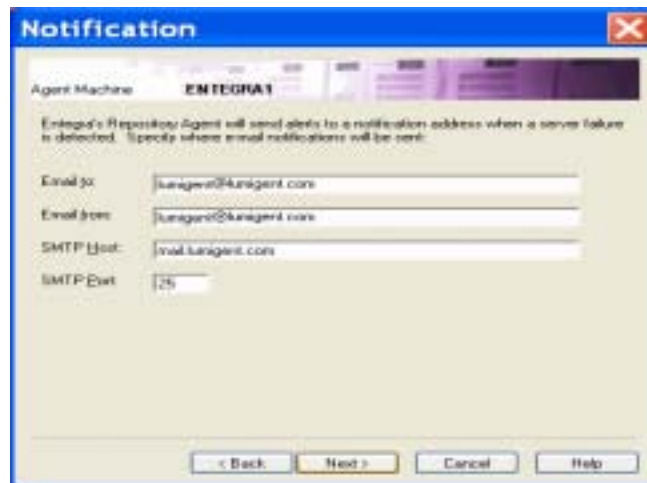
Note: Select the local system account if you used a database logon on the previous screen. Specify a Windows login if you specified Windows logon on the previous screen. This account is used to log on to the Repository during Import operations.

The “Archive” screen is displayed.



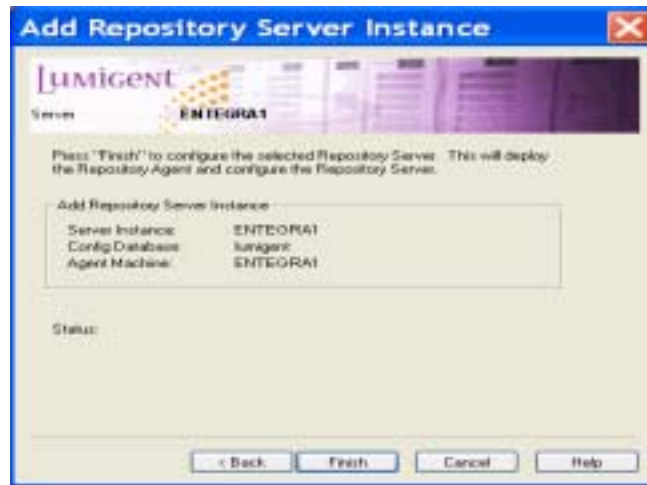
5. Specify the directory for the archive files to be stored, and then click **Next**.

The “Notification” screen is displayed.



6. Type the notification address where you want alerts sent when a server failure is detected, and then press **Next**.

The screen that allows you to complete the configuration wizard is displayed.



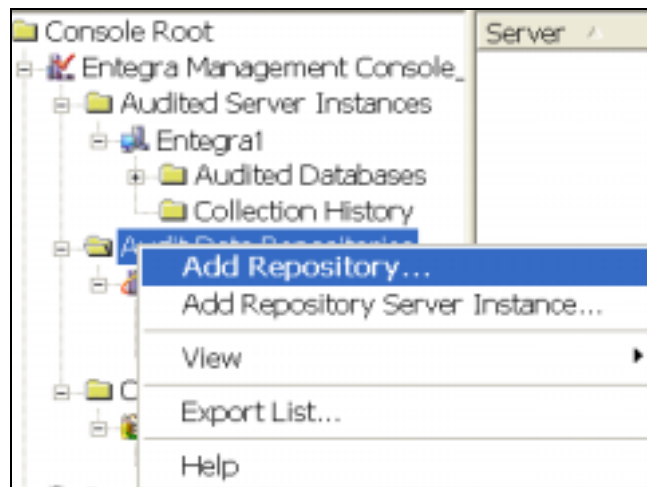
7. Click **Finish**.

The Repository Agent is deployed and the Repository Server is configured.

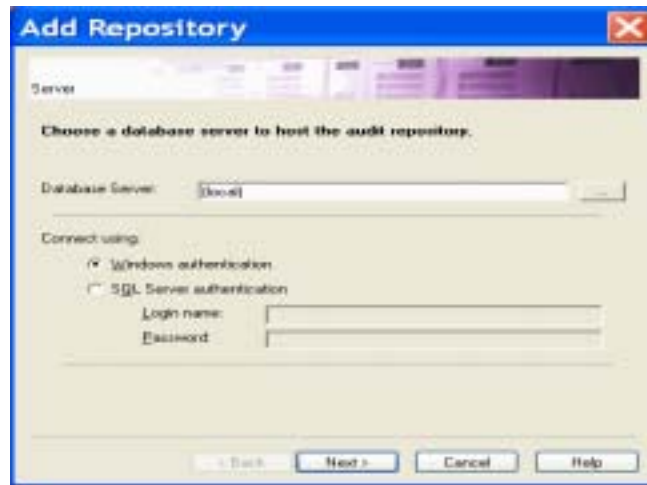
## Adding a Repository


To add a Repository, do the following:

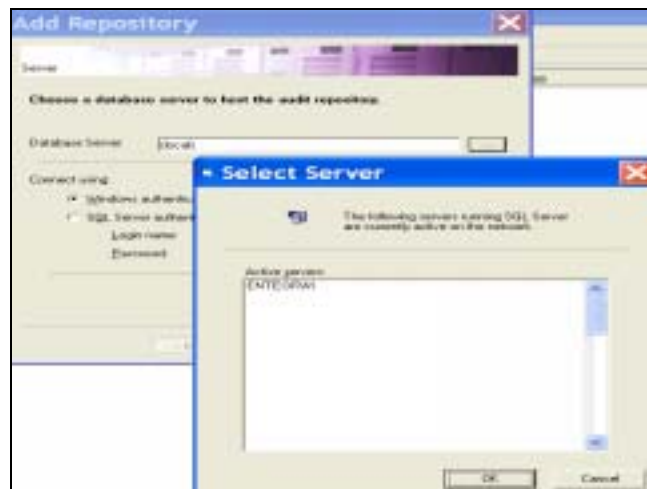
1. At the EMC, right-click **Audit Data Repositories**, and then click **Add Repository**.



The “Add Repository” Wizard is displayed.



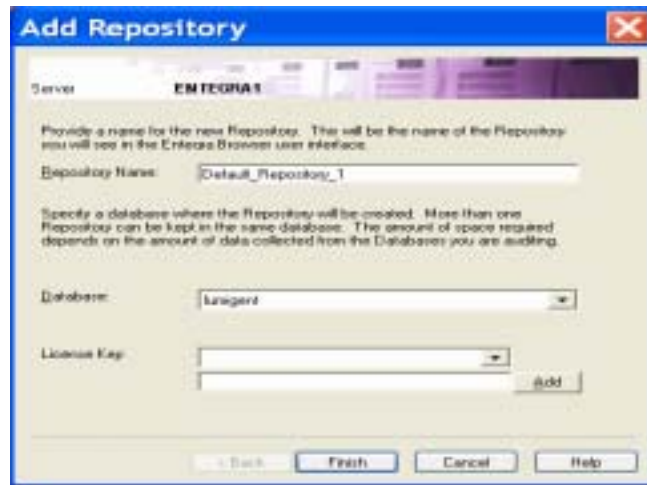
2. In the **Database Server** text box, type the database server you want to audit, or click the browse button  to display the available database servers as shown below. Select from the available database servers, and then click **OK**.



3. If you want to connect using SQL Server authentication, click the **SQL Server authentication** radio button, enter a logon name and password, and then click **Next**.

Note: If a repository server has not been established on this server, the “Service Log On” screen from the Repository Server wizard is displayed. Go to step 3 in *Adding a Repository Server Instance* wizard and continue.

The screen that allows you to complete the configuration wizard is displayed.

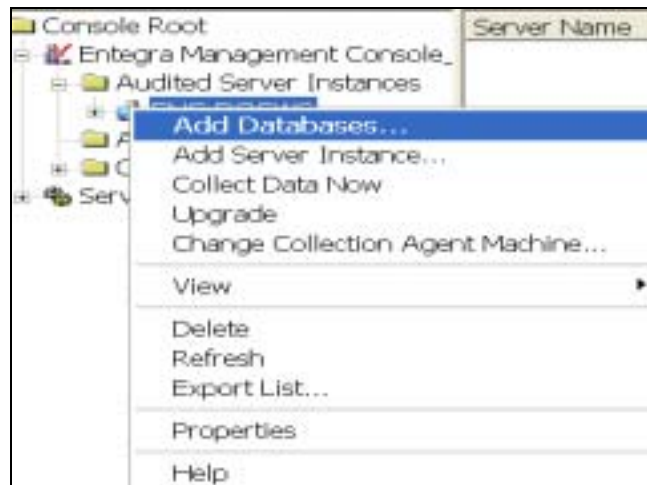


4. Provide a name for the new repository, specify a database for the new repository, and add the license key, and then click **Finish**.

## Adding a Database to Audit

To add at least one database to audit, do the following:

1. At the EMC, right-click the relevant audited server, then click **Add Databases**.



The “Add Databases to Audit” wizard is displayed.

Important: Do not select the database that is used as a repository for the audited data. If you audit the repository tables, it sends the audit data to the repository causing the repository to grow at a rapid rate.

If you wish to audit the repository database, set up a separate repository to hold the contents of that audit data.



2. Select the databases you wish to audit from the **Available Databases** window, and click the right-arrow button to move them to the **Target Databases** window, and then click **Next**. Click the **All** box to quickly select all databases.

The screen with the databases that you selected to audit is displayed.

Note: Only newly selected databases are displayed; databases that are already set up for audit are not displayed.



3. If you do not wish to audit all tables, clear the **Enable Data Modification auditing on all tables** check box.

Note: If you clear the **Enable Data Modification auditing on all tables** check box, you must manually specify tables to audit after you complete the Add Database wizard. (See Add or Remove Tables.)



4. If you want to enable SELECTs auditing on all tables and views and the check box is available, select the **Enable SELECTs auditing on all tables and views** check box.

Note: The SELECTs check box is not displayed for SQL Server 7 servers.

5. If you are certain that the logs for this database are not kept in the default SQL Server directory, enter the appropriate directory in the **Backup log path** field; otherwise, use the default.

Note: This backup log path is used for all the databases displayed on this page. If these databases use different backup log paths, then add them separately. You can also access the properties of each database after they are added to enter the correct directory for each database.

Recommendation: It is recommended that the database's online log be kept in a directory separate from the backup log directory.

6. At the **Post Processing** drop-down box, click the down arrow and select an option for how the database logs should be handled after Entegra finishes collecting data from them.

Note: Entegra provides the following options for what to do with the backup log after the audit data has been harvested:

- Leave the log in the backup directory (default)
- Rename the log to a post processing directory
- Delete the log

Entegra ignores logs that it has already processed. See Chapter 4 for details.

7. If you select **Rename the log to the post processing directory**, then at the **Post Processing Directory:** field, enter the path name to the directory.
8. Click **Next**.

If you have...	Then...
already added a repository	the following screen is displayed.
not yet added a repository	the Add Repository Wizard is displayed. Refer to the Adding a Repository Server Instance procedure for details.



9. Select the default repository by clicking **Next**, or click the **Create New Repository** button. (See the Adding a Repository Server Instance procedure.)

The screen with the names of the databases to be audited and the repository is displayed.



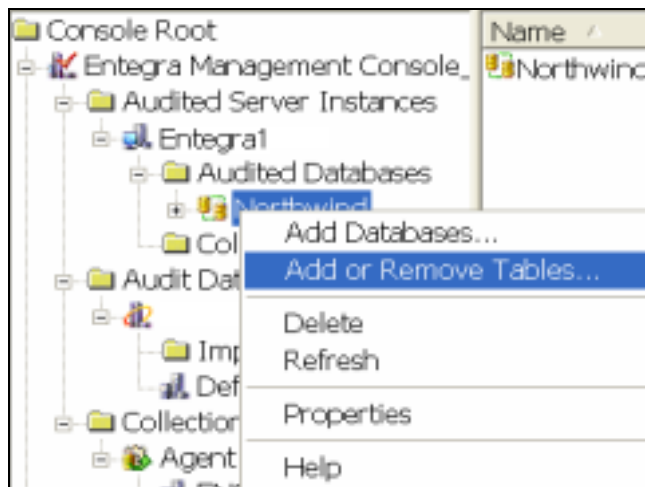
10. Click **Finish** to add the databases to the audit.

## Adding/Removing Tables

To add or remove multiple tables, see the section, *Audit Settings for Multiple Tables*.

To add or remove all or selected tables, do the following:

1. At the EMC, right-click an audited database, and then click **Add or Remove Tables**.



The “Add or Remove Tables” wizard is displayed.

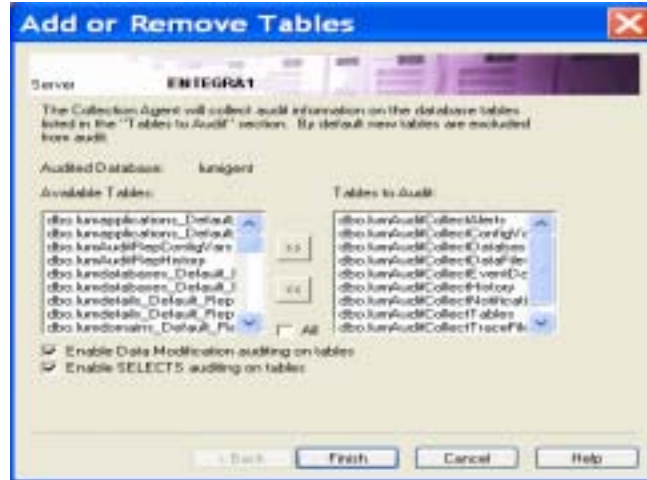
Enabling the **Data Modification auditing on tables** option audits the table for the following operations:

- INSERT
- UPDATE
- DELETE

Note: A DML license for the server is needed for this option.

Enabling the **SELECTs auditing on tables** option audits the table for SELECT operations. A SELECTs license for the server is needed for this option.

The **Tables to Audit** window on the right displays the tables that are currently selected for auditing, and the **Available Tables** window on the left lists tables in the database that are not selected for auditing.



2. Select the tables you wish to move and use the right arrow and left arrow buttons to move tables from one window to the other. You can click the **All** box to quickly select all tables in a window. When you are finished making selections, click **Finish**.

Note: By default, all columns in a table are audited. If you wish to exclude certain columns from auditing, see *Add/Remove Columns to Audit*.

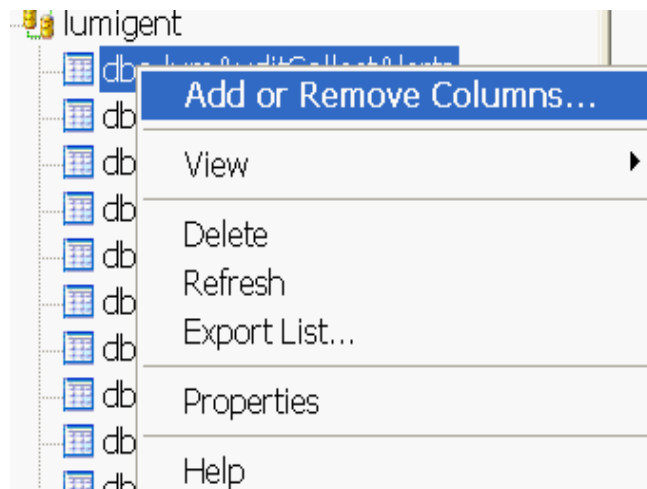
By default, the logical key is automatically selected for each table. To select the logical key, see *Selecting the Logical Key*.

## Selecting Audit Settings for Individual Tables

To change audit settings for an individual table, do the following:

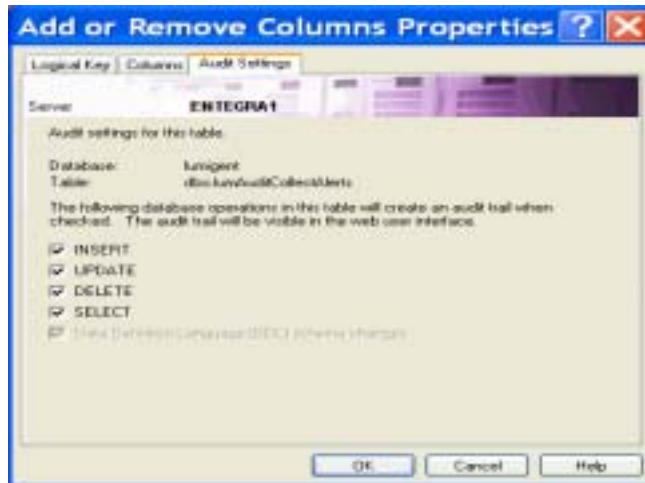
1. Right-click the relevant audited table, and then select **Add or Remove Columns**.

The “Add or Remove Columns Properties” screen is displayed.



2. Select the **Audit Settings** tab.

The audit setting check boxes are displayed.



3. Make your selections and then click **OK**.

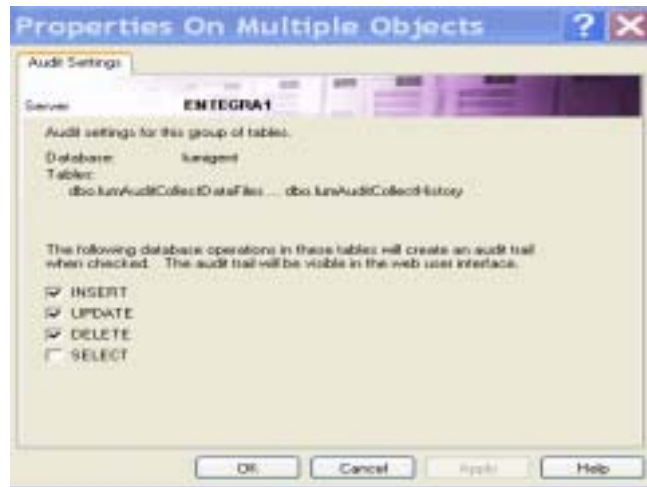
## Selecting Audit Settings for Multiple Tables

You can set the audit settings for multiple tables by doing the following:

1. At the EMC, expand the audited database to display the tables in the results pane.
2. Use **Shift+click** or **Ctrl+click** to select more than one table, right-click the selections, and then select **Properties**.

Table Name	Audit Type	Columns being audited
dbo.lumAuditCollectAlerts	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectConfigVars	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectDatabases	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectDataFiles	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectEventData	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectHistory	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectNotification	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectTables	INSERT;UPDATE;DELETE	*
dbo.lumAuditCollectTraceFiles	INSERT;UPDATE;DELETE	*

The “Properties on Multiple Objects” screen is displayed.

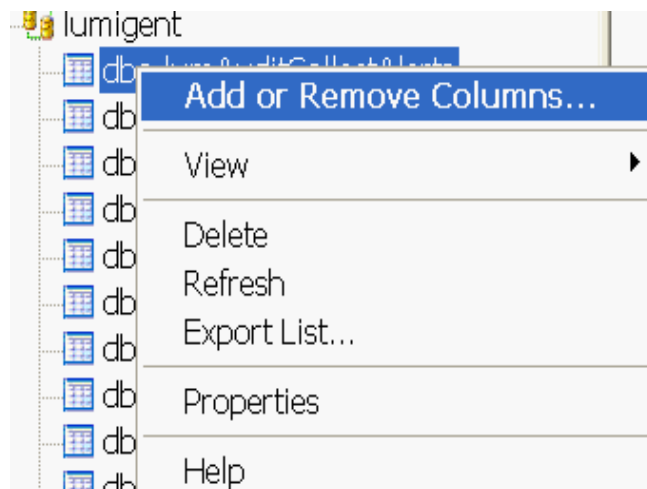


3. Make your selections, and then click **OK**.

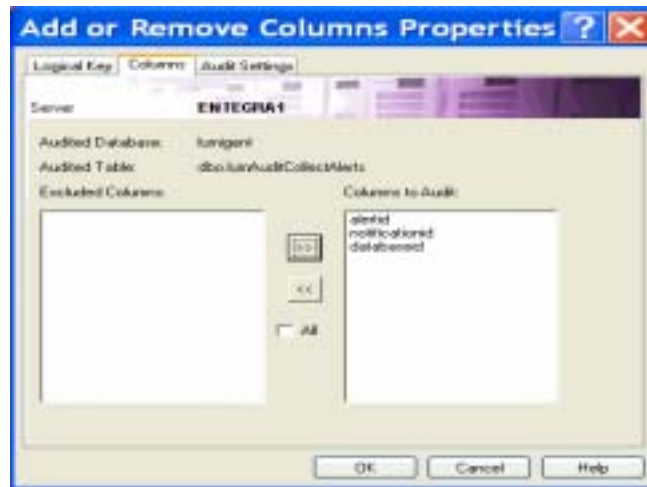
## Adding/Removing Columns

By default, all columns in a table are audited. Removing columns may reduce the storage required for the repository and improve performance. If you wish to add or remove columns from auditing, do the following:

1. Right-click the relevant audited table, and then select **Add or Remove Columns**.



The “Add or Remove Columns Properties” screen is displayed.

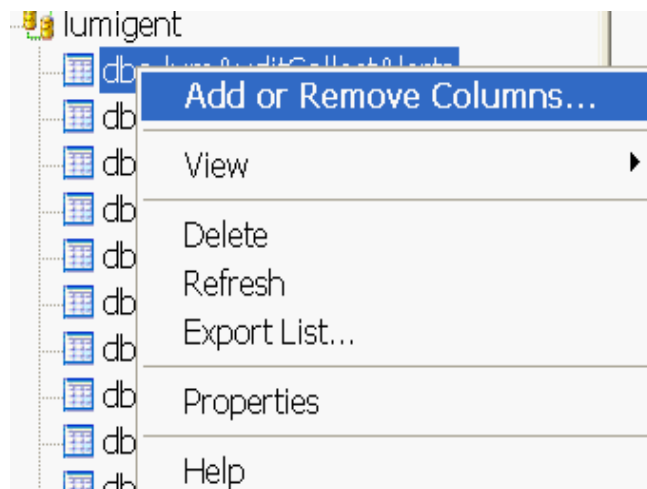


2. Select the columns you wish to move and use the right arrow button to add columns to audit; use the left arrow button to remove columns from audit, and then click **OK**. You can click the **All** box to quickly select all columns.

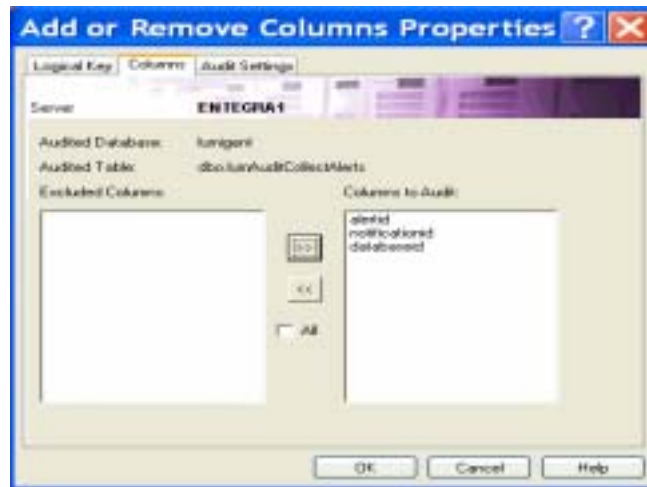
## Selecting the Logical Key

To select the logical key, do the following:

1. Right-click the relevant audited table, and then select **Add or Remove Columns**.

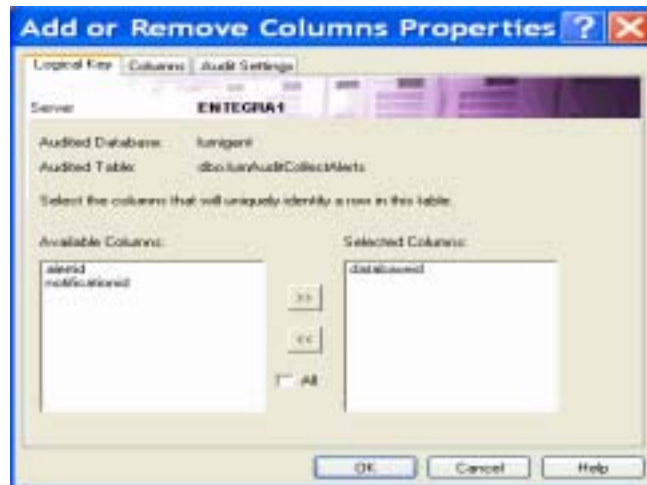


The “Add or Remove Columns Properties” screen is displayed.



2. Select the **Logical Key** tab.

The available and selected logical key columns are displayed.



3. Select the columns you wish to define as logical keys and use the right arrow button to add the logical keys; use the left arrow button to remove the logical keys, and then click **OK**. You can click the **All** box to quickly select all columns.

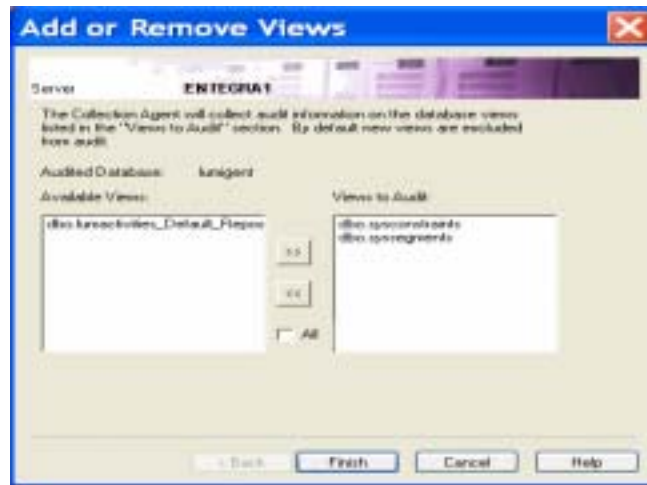
## Adding/Removing Views

Note: This wizard is not available on SQL Server 7 servers.

To add a database view to the collection agent, do the following:

1. Right-click the relevant database, and then select **Add or Remove Views**.

The “Add or Remove Views” screen is displayed.



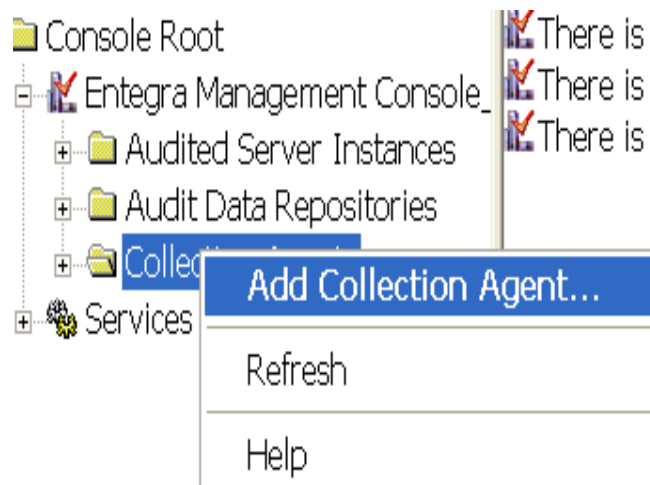
2. Select the views you wish to move and do the following:
  - to add views, use the right arrow button to add your selections to the **Views to Audit** window.
  - to remove views, use the left arrow button to move your selections to the **Available Views** window.
3. Click **Finish**.

Tip: You can click the **All** box to quickly select all views.

## Adding a Collection Agent

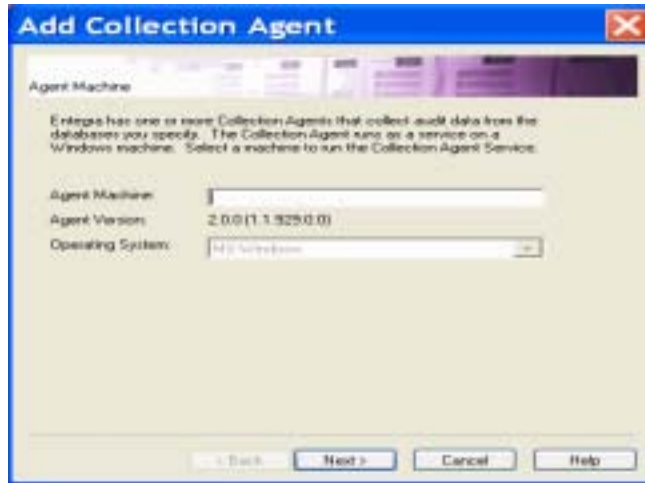
To add a collection agent, do the following:

1. At the EMC, right-click **Collection Agent**, and then click **Add Collection Agent**.



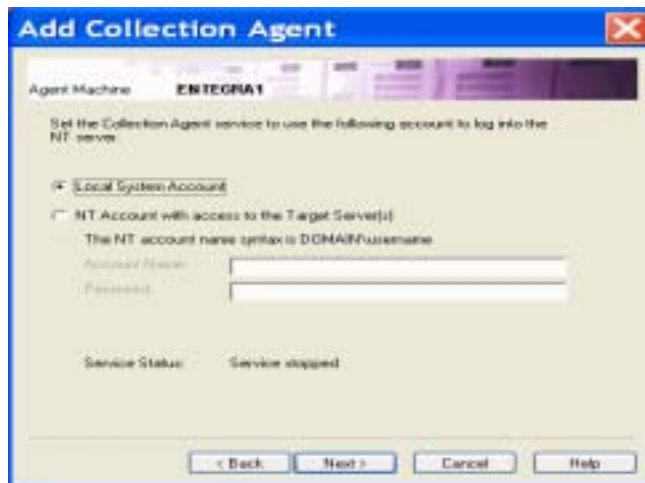


The “Add Collection Agent” wizard is displayed.



2. Specify the location (machine name) where you want to install a Collection Agent, and then click **Next**.

The screen that allows you set the collection agent service is displayed.



For this screen, you need to consider the following:

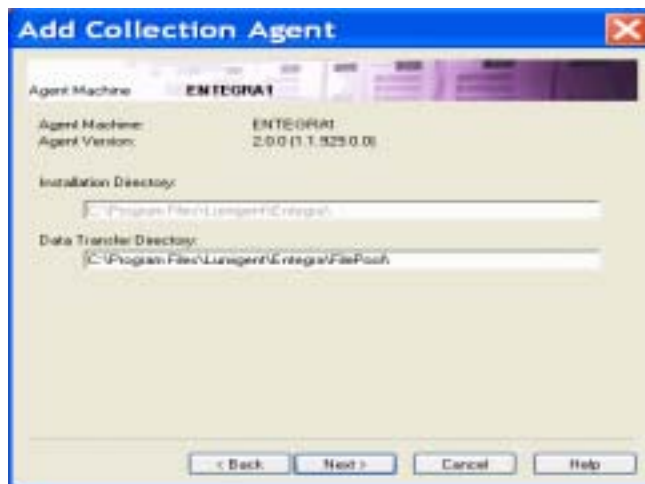
If you want the Audited Server and the Collection Agent...	Then...
on the same machine	you can use the database logon for the server and local service login for the agent or, you can use Windows logon for both the audited server and the agent.
each on a different machine	it is highly recommended that you use Windows logon for the audited server and the agent.  Note: The Windows account used to log on to the Audited Server is specified on the Agent log on page.

- Specify the account for the Collection Agent service to use to log on to the NT server, and then click **Next**.

Note: The log on you use must have "Logon as Service" privileges on the Agent machine. If you choose a log on name that does not have the necessary privileges, you receive a "logon failed" error message.

The screen that allows you to select a storage directory is displayed.

Note: If the Installation Directory location box is not available, then there is already an Entegra component installed on that machine. Entegra installs all of its components to the same directory on a given machine.



The Data Transfer Directory is the directory where the Agent stores audit data files prior to transmitting them to the Repository Agent.

- Specify the Data Transfer Directory where you want the Agent to store audit data files prior to transmitting them to the Repository Agent, and then click **Next**.

The screen that allows you to type your email information for server failure notification is displayed.

The screenshot shows a Windows-style dialog box titled "Add Collection Agent" with a blue header bar and a red close button. The main content area has a light beige background. At the top, it says "Agent Machine: INTEGRAL". Below that, a message states: "Entegri's Collection Agent will send alerts to a notification address when a server failure is detected. Specify email configuration:". There are four text input fields: "Email to:" with "lunigent@lunigent.com", "Email from:" with "lunigent@lunigent.com", "SMTP Host:" with "mail.lunigent.com", and "SMTP Port:" with "25". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

5. Specify your email information for failure notifications, and then click **Next**.  
The screen that allows you to complete the configuration wizard is displayed.

The screenshot shows the same "Add Collection Agent" dialog box, but now it features the "Lunigent" logo at the top left. The text in the center says: "Press 'Finish' to establish an Agent on the following machine:". Below this, it lists "Agent Machine: INTEGRAL". At the bottom, the buttons are "< Back", "Finish", "Cancel", and "Help".

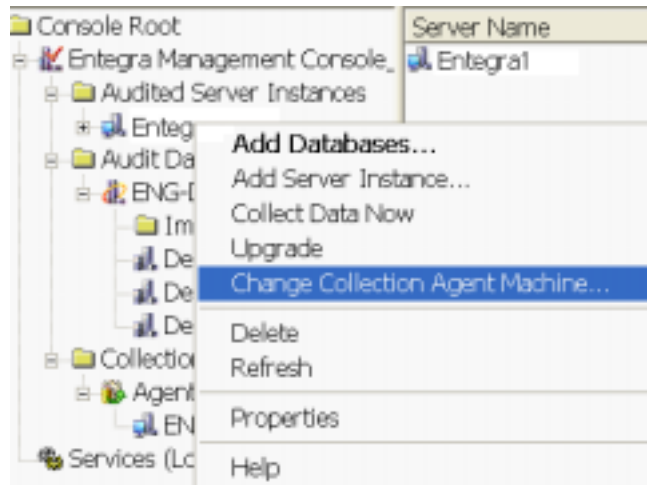
6. Click **Finish** to create the new Agent, or click the **Back** button to change options.

## Changing a Collection Agent

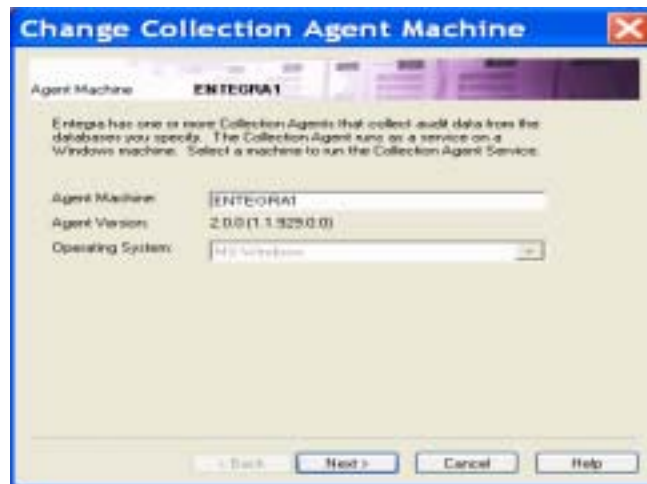
This is not a wizard that is generally run as part of initial configuration. You may want to change a collection agent if Entegra collections are negatively affecting performance on a production machine and you want to move this workload to a different machine. In this case, the Change Collection Agent wizard smoothly transfers the workload from the old machine to the new machine. It is best to do this when no collections are taking place

To change a Collection Agent, do the following:

1. At the EMC, right-click the relevant audited server instance, and then click **Change Collection Agent Machine....**

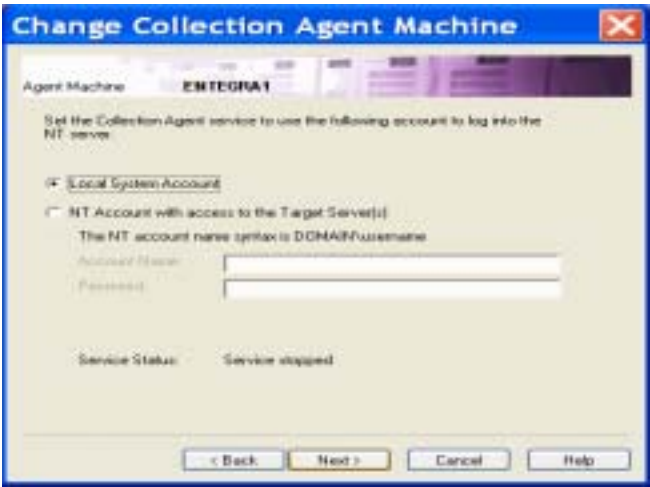


The “Change Collection Agent Machine” wizard is displayed.



2. Type the name of the new machine that you want to run as the Collection Agent Service, and then click **Next**.

The screen that allows you set the collection agent service is displayed.



For this screen, you need to consider the following:

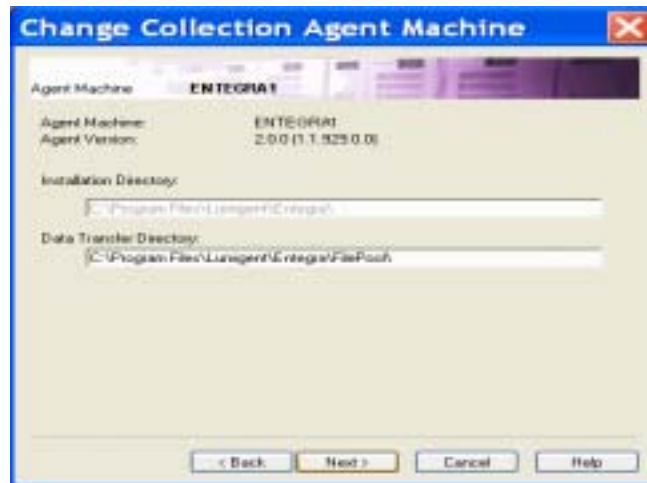
If you want the Audited Server and the Collection Agent...	Then...
on the same machine	you can use the database logon for the server and local service logon for the agent or, you can use Windows login for both the audited server and the agent.
each on a different machine	it is highly recommended that you use Windows logon for the audited server and the agent.  Note: The Windows account used to log on to the Audited Server is specified on the Agent logon page.

3. Specify the account for the Collection Agent service to use to log on to the NT server, and then click **Next**.

Note: The logon you use must have "Logon as Service" privileges on the Agent machine. If you choose a logon name that does not have the necessary privileges, you receive a "logon failed" error message.

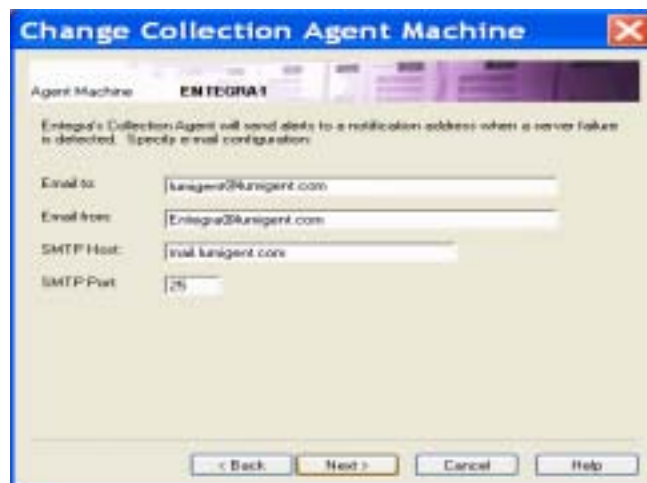
The screen that allows you to select a storage directory is displayed.

Note: If the Installation Directory location box is not available, then there is already an Entegra component installed on that machine. Entegra installs all of its components to the same directory on a given machine.



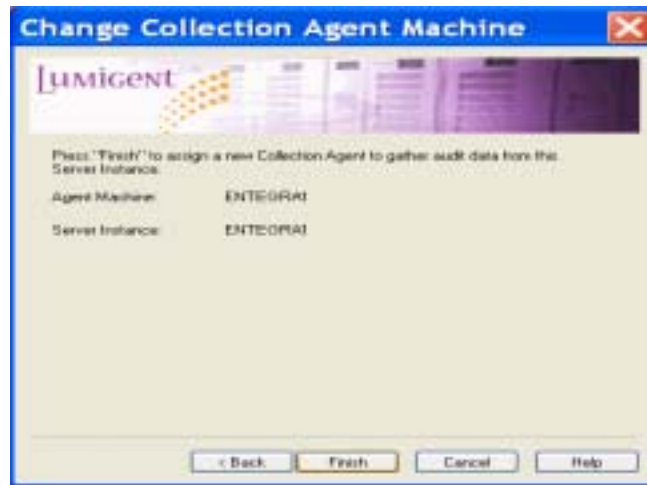
4. Specify the Data Transfer Directory where you want the Agent to store audit data files prior to transmitting them to the Repository Agent, and then click **Next**.

The screen that allows you to type your email information for server failure notification is displayed.



5. Specify your email information for failure notifications, and then click **Next**.

The screen that allows you to complete the configuration wizard is displayed.



6. Click **Finish** to create the new Agent, or click the **Back** button to change options.

## Using Multiple Entegra Management Consoles

It is recommended that you use only a single console to administer your Entegra configuration. If you use multiple consoles, you must adhere to the following guidelines.

You can install and run the Entegra Management Console on multiple machines to manage separate Entegra environments as long as the multiple EMC's are not auditing the same servers.

**Caution:** In cases where Entegra administrators are using multiple consoles, be aware that the configuration may get into an unexpected state if administrators operate on the configuration for the same component at the same time. This outcome is most likely to occur if the console property pages are kept up for long periods of time (hours, days) before being committed.

## Configuration Examples

This section includes examples of typical configurations. These examples are intended as an introduction to the configuration process; they may not precisely match the steps you take, but they provide an overview on how you might proceed.

### Using Online Help

On any given screen in the Entegra Management Console, you can click the **Help** button for assistance with that particular screen.

## Example 1

Example 1 provides a basic configuration example in which you have one server being audited and a separate server running all the remaining Entegra components – the Agents, the Management Console, the Web Server, and the Repository.

## Example 2

Example 2 provides a high-security example. A single server contains two databases – Payroll and Customers – each with its own logon username and password. A second server contains two Repositories, one for each database. For additional security, this configuration also uses a third machine as the Web Server.

## Example 3

Example 3 provides a scaled enterprise example consisting of two databases on two different servers, both handled by a single Collection Agent on one of the servers, with both databases' data going to a single Repository on a third server.

## Example 4

Example 4 provides a cluster example. A SQL Server instance that is being audited is part of a cluster. This example assumes that the Audited Server Instance resides on the active node of an active/passive cluster. All other components – the Entegra Management Console, Collection Agent, Repository, Repository Agent, and Web Server – reside on a separate machine outside the cluster. This configuration is exactly the same as Example 1.

# Example 1: Setting up two machines as an Entegra environment

Example 1 presents the process of setting up two machines as an Entegra environment. The first machine to configure, called SERVER1, is a SQL Server machine running a production database. The second machine, called ENTEGRA1, is dedicated to the Entegra software.

This example takes you through the following stages:

Stage	What Happens
1	Prerequisites and installation.
2	Add an Audited Server Instance and deploy Agents.
3	Specify databases to audit.

## Prerequisites and installation

To ensure that the prerequisites for installation are met and to install Entegra software, do the following:

1. Ensure that both machines meet the hardware, software/operating system, and network connectivity requirements described in Chapter 2.



2. Ensure that login names and passwords are available that fit the criteria described in the "Security" section of Chapter 2. For the purpose of this example, Windows authentication is used throughout the system.
3. Log on to ENTEGRA1 using a Windows login that has full administrative privileges on the machine.
4. Using the provided media, install the Entegra Management Console and Web Server on ENTEGRA1.

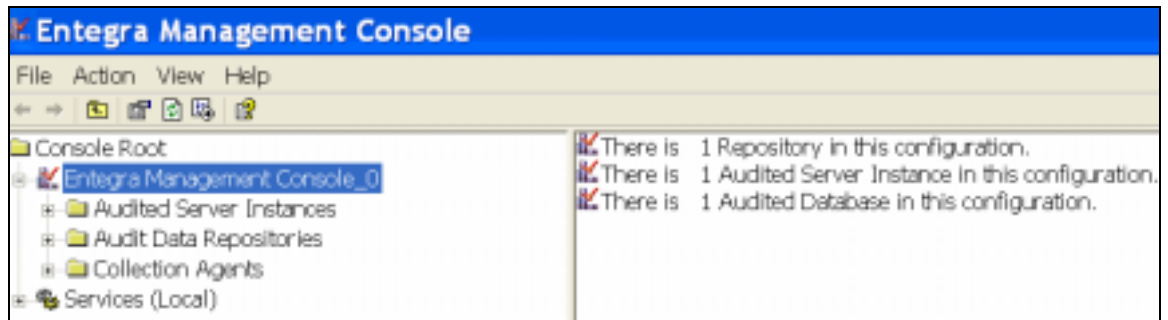
This concludes the installation portion of the setup process. Next, SERVER1 is set up as an Audited Server Instance, and Agents are deployed.

## Add an Audited Server Instance, and deploy Agents

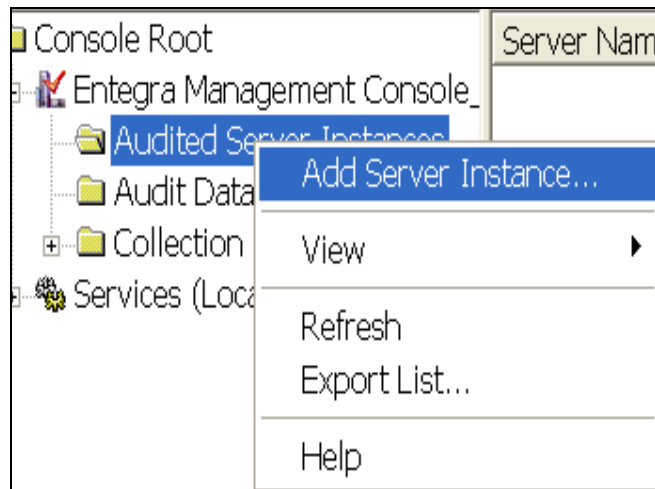
To add an Audited Server Instance, and deploy Agents, do the following:

1. Launch the Management Console from the desktop shortcut or the Start Menu (*Start, Programs, Lumigent, Entegra, Management Console*).

The initial screen resembles the following:



2. Right-click **Audited Server Instances**, and then select **Add Server Instance**.

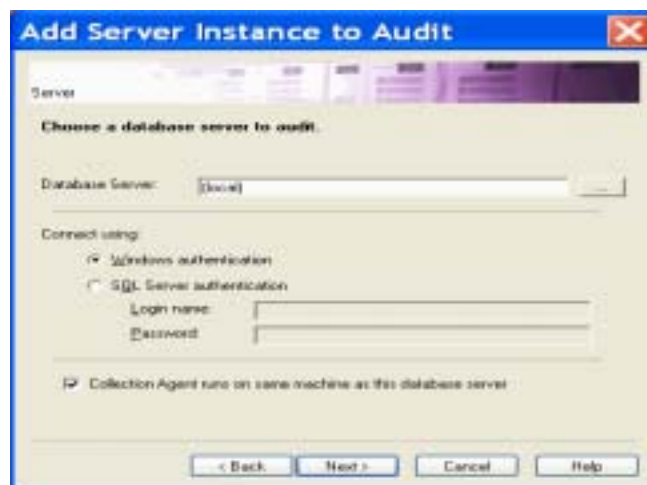


The “Add Server Instance to Audit” wizard is displayed.

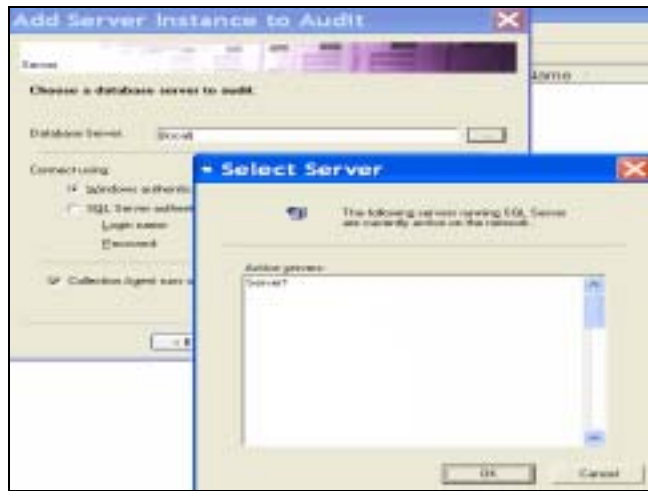


3. Click **Next**.

The screen where you choose a database server to audit is displayed.



4. In the Database Server text box, type SERVER1, or click the browse button ... to display the available database servers as shown below. Select SERVER1, and then click **OK**.



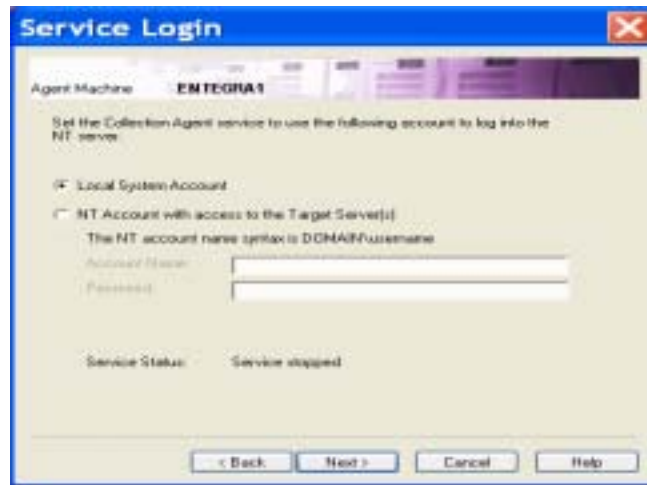
5. Select the **SQL Server authentication** radio button, enter the username and password for a SQL login account that has sysadmin privileges on ENTEGRA1, clear the **Collection Agent runs on the same machine as this database server** check box, and then click **Next**.

The screen that allows you to add a machine for the collection agent is displayed.



6. In the **Agent Machine** text box, type ENTEGRA1, and then click **Next**.

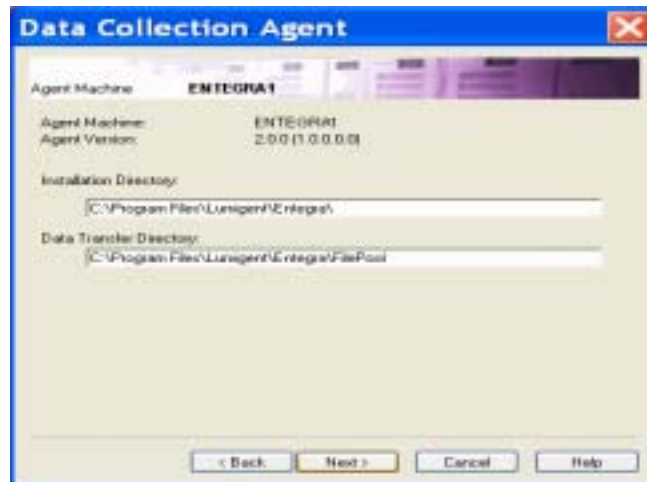
The “Service Login” screen is displayed.



This screen asks for login information that the Collection Agent uses to run its service.

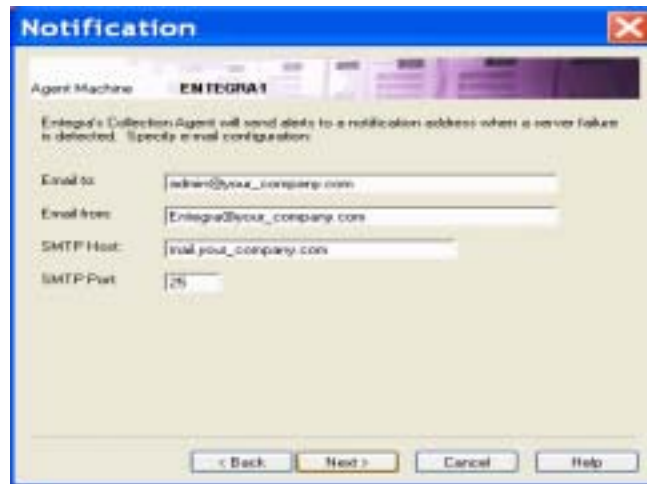
7. Select the **NT Account with access to the Repository Server Instance(s)** radio button and type the Account Name and Password, and then click **Next**.

The “Data Collection Agent” screen is displayed.



8. Select the locations where you want the Collection Agent installed and where you want it to store its audit data files, and then click **Next**.

The “Notification” screen is displayed.

The "Notification" window has a blue title bar with the text "Notification" and a close button. Below the title bar is a tabbed interface with the "SERVERS" tab selected. The main area contains the text: "Entegra's Collection Agent will send alerts to a notification address when a server failure is detected. Specify email configuration:". There are four text input fields: "Email to:" with the value "admin@your\_company.com", "Email from:" with the value "Entegra@your\_company.com", "SMTP Host:" with the value "mail.your\_company.com", and "SMTP Port:" with the value "25". At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

9. Enter email information for the Collection Agent to use when emailing you about collection failures. You must enter a To and From email address, and the name of your mail server, and then click **Next**.

The screen that allows you to select your license capabilities is displayed.

The "Add Server Instance to Audit" window has a blue title bar with the text "Add Server Instance to Audit" and a close button. Below the title bar is a tabbed interface with the "SERVERS" tab selected. The main area contains the text: "The capabilities you have available are displayed in the list below. You can add additional capabilities by entering a valid license key." and "Check the capabilities to be assigned to this server:". There is a list box containing two items: "DCL" and "Modifications". The "Modifications" item is selected, indicated by a checkmark in a box to its left. Below the list box is a text input field for "License Key:" and an "Add" button. At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

10. Type or paste the license key into the **License Key** text box and click **Add**.  
All Entegra features available in this key are displayed in the window.
11. Check the boxes next to the features that you wish to enable for this audited server instance, and then click **Next**.

The screen that allows you to set auditing frequency is displayed.



12. Set the schedule for automatic collection.

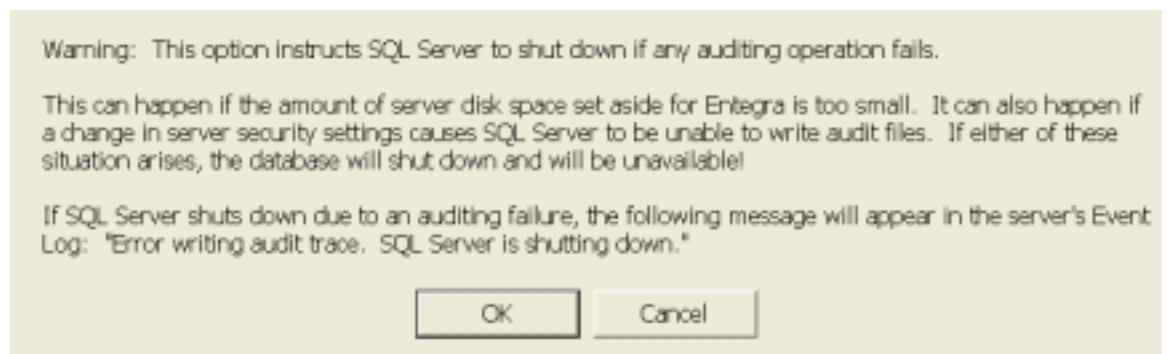
Recommendation: Schedule collections for low-traffic times of day. Also, avoid overlap of collection and backup operations. Ideally, collections should be run shortly after the backup completes.

For this example, set the collection schedule to 7:00 A.M and 7:00 P.M. every day. To do so, click the arrow:

- a. In the Start Date box, select tomorrow's date.
- b. In the Start Time box, select 7:00 A.M.
- c. In the Frequency section, change the units to "hours" and enter 12 in the text box.

13. To choose the option, **Shutdown the server on audit error to protect audit integrity**, select the check box, and then click **Next**.

Note: If you select this option, the following warning is displayed:



14. Click **OK** to accept this option, or click **Cancel** to clear it.

The screen that allows you to specify how alerts are sent from the server is displayed.

The screenshot shows the 'Add Server Instance to Audit' dialog box with the title bar in blue. The main area has a light yellow background. At the top, it says 'Server: SERVER1'. Below that, a text box explains: 'Specify how alerts will be sent from this server. The next page will let you select which events generate alerts. If you do not want any alerts generated, clear both the email and event log check boxes.' There are two checked checkboxes: ☒ 'Add alert events to the event log on this server' and ☐ 'Email to:'. Below the email checkbox are three text boxes: 'Email to:' (containing 'Lunagard@lunagard.com'), 'Email from:' (containing 'Lunagard@lunagard.com'), and 'SMTP Host:' (containing 'mail.lunagard.com'). There is also an 'SMTP Port:' field with '25' entered. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

This optional feature alerts you any time an event of a specified type occurs. (You specify the types of events that trigger alerts in the next step.) By default, alerts are logged to the Windows Event Log on the local server.

15. Select the methods by which you want to be notified when an alert condition occurs. To have alert events emailed, select the **Email to:** check box, make any modifications in the text boxes, and then click **Next**.

The screen that allows you to select alert events is displayed.

The screenshot shows the 'Add Server Instance to Audit' dialog box with the title bar in blue. The main area has a light yellow background. At the top, it says 'Server: SERVER1'. Below that, a text box explains: 'An alert will be generated each time a selected event occurs in an audited database on server SERVER1.' There are several checked checkboxes: ☒ 'Create, Drop Database', ☒ 'Create, Alter, Drop Objects other than databases', ☒ 'Grant, Deny, Revoke Permissions', ☒ 'Add, Remove Login', ☒ 'Add, Remove User', ☒ 'Add, Remove Role', ☒ 'Restore Database', ☒ 'Failed login', and ☒ 'Successful login'. There are also unchecked checkboxes: ☐ 'Include Create, Alter, Drop of Temporary Tables', ☐ 'Database Console Command (DBCC)', ☐ 'Backup Database', and ☐ 'Logout'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

16. Select database events that you wish to be alerted of in real-time, and then click **Next**.

Important: Selecting the **Successful login** option generates a large number of alerts. If these alerts are emailed to you, server performance may be impacted.

The screen that allows you to complete the configuration wizard is displayed.



17. Click **Finish** to complete the installation.

Entegra installs the Collection Agent on ENTEGRA1, and installs necessary components on SERVER1.

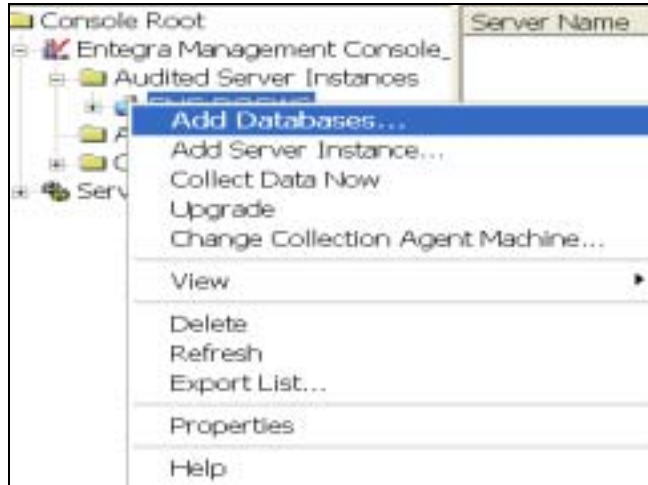
You have now finished setting up SERVER1 as an Audited Server Instance and deploying Agents. Next, you must add databases to audit.



## Add a Database to Audit


To add at least one database to audit, do the following:

1. Using the Entegra Management Console, expand **Audited Server Instances** and right-click SERVER1, and then select **Add Databases**.



The “Add Databases to Audit” wizard is displayed.



2. Select the databases you wish to audit from the **Available Databases** window, and click the right-arrow button  to move them to the **Target Databases** window, and then click **Next**. Click the **All** box to quickly select all databases.

Tip: You can also double-click databases to move them.

The screen with the databases that you selected to audit is displayed.

Note: Only newly selected databases are displayed; databases that are already set up for audit are not displayed.



3. Ensure that the **Enable Data Modification auditing on all tables** check box is selected.

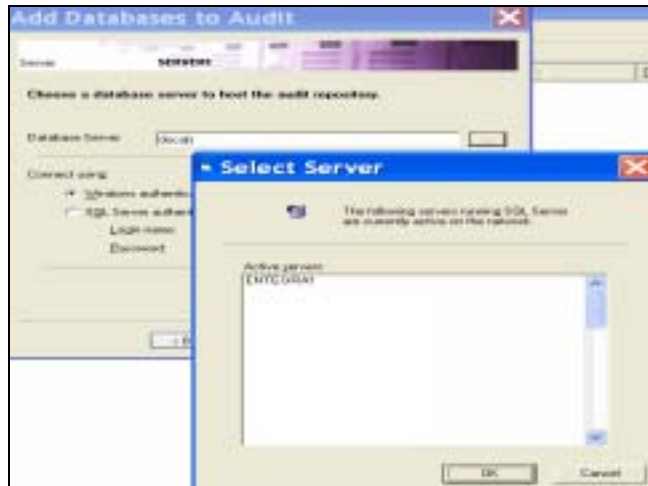
If you are certain that the backup log for the selected databases is not in the SQL Server default location, enter it in the **Backup log path** box; otherwise leave the default. (For a full explanation of the other options on this screen, see Chapter 4.)

4. If available, select the **Enable SELECTs auditing on all tables and views** check box, and then click **Next**.

Since you have not yet created a Repository, the Repository Server Instance wizard is incorporated into the Add Database wizard.

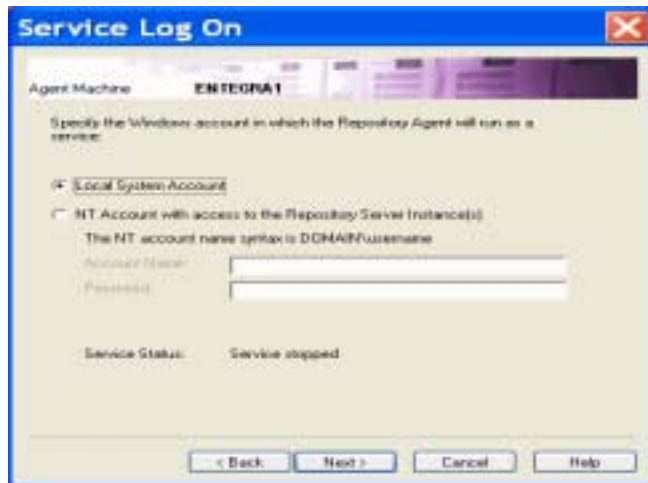


5. In the **Database Server** text box, type ENTEGRA1, or click the browse button **...** to display the available database servers as shown below. Select ENTEGRA1, and then click **OK**.



6. Click **Next** to accept the default of the currently logged-on account. (Alternatively, you may enter a valid SQL Server database login name and password.)

The "Service Log On" screen is displayed.

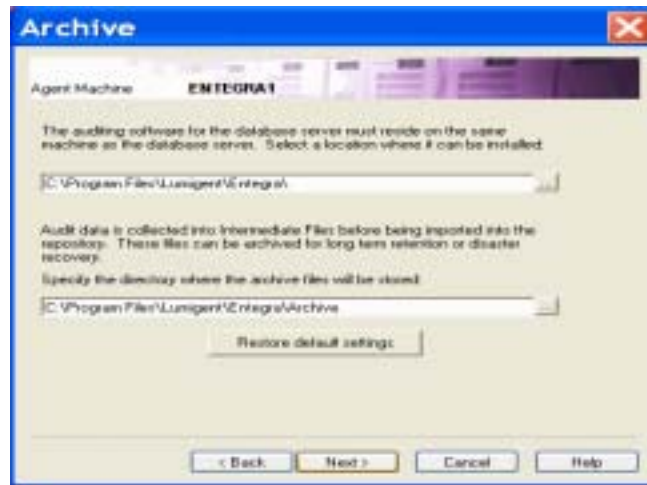


The Service Log On screen information is used by the Repository Agent to run its service.

7. Leave all fields blank and click **Next**, to use the local system account. Alternatively, you can specify a username and password.

This account must have "logon as service" permission on ENTEGRA1.

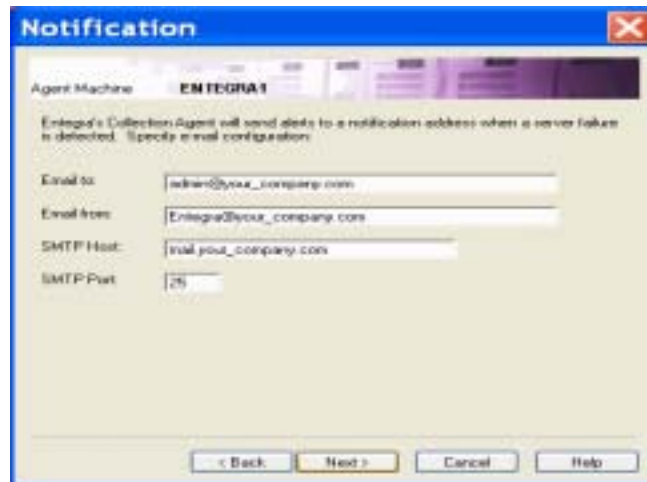
The “Archive” screen is displayed.



8. Select a location for audit data to be archived after it has been imported into the Repository, and then click **Next**.

For further details on this feature, see Chapter 4.

The “Notification” screen is displayed.



9. Enter email information for the Repository Agent to use when emailing you about import failures, and then click **Next**.

The following screen is displayed.

You have the option of selecting a name for the Repository. By default, it is called "Default\_Repository."

10. Type a new Repository name, or keep the default, and then click **Next**. (You can also select an alternate database for the Repository to reside in. By default, it is installed in the lumigent database.)

Restriction: Using a non-alphanumeric character as the first character of a repository name can cause problems. Use an alphanumeric character to begin a repository name. You may use special characters (the following are accepted: @ \_ \$ #) elsewhere in the repository name.

This screen allows you to specify a Repository license key. If the license that you entered during the Add Audited Server Instance Wizard included Repository capabilities, it is displayed here and can be used for the Repository you are now creating. If not, you must enter a valid Repository license key before continuing.

The screen that allows you to complete the configuration wizard is displayed.

11. Verify that all your selections are correct, and click **Finish**.

The Repository is set up, the Repository Agent is deployed, and the selected databases are set to be audited.

You have now finished configuring your Entegra environment. Automatic collection of audit data occurs according to the schedule you selected.

12. To start collecting data immediately, select the Audited Server Instance, right-click and then select **Collect Data Now**.

Note: The first collection may take a long time if there is a large amount of historical data for the databases being audited. Entegra collects audit data from all of the transaction logs and log backups that are available in the directories you specified.

You can check on the progress of the auditing process by selecting any of the following nodes in Entegra and pressing the **F5** (Refresh) key:

- Collection History, under the Audited Server Instance
- Import History, under the Repository Server Instance
- Databases folder, under the Audited Server Instance

When the Import is complete, your users can access the Entegra Browser by using the installed desktop shortcuts or by connecting to

<http://ENTEGRA1:8080/umi gent/ l ogi n. html> and logging in with the appropriate permissions (see Chapter 6).

Optionally, you can now fine-tune your configuration by doing any of the following:

- selecting which tables to audit (see Add or Remove Tables)
- selecting which columns to audit (see Add or Remove Columns)
- selecting logical keys for tables (see Selecting the Logical Key)

## Example 2: Setting up a distributed Entegra environment on three machines

In Example 2, you set up a distributed Entegra environment on three machines. An existing SQL Server machine called SERVER1 holds two important databases, Payroll and Customers, each with its own security information.

A second machine, ENTEGRA1, receives the audit data and stores it in a local repository, while a third machine, ENTEGRA2, runs the Web Server. The Entegra Management Console runs on ENTEGRA1.”

ENTEGRA1 hosts two repositories, one for audit data from the Payroll database, and one for audit data from the Customers database. (Maintaining separate repositories allows the administrator to apply different permissions to each for greater security.)

In this setup, you install the Collection Agent on the Audited Server Instance SERVER1 for convenience. (On high-volume systems you can run the Collection Agent on a machine other than the Audited Server Instance, as shown in Example 1. The Collection Agent may cause slight performance degradation on the server machine.)

This example takes you through the following stages:

Stage	What Happens
1	Prerequisites and installation.
2	Add an Audited Server Instance and deploy Agents.
3	Create a Payroll Repository and create a Customer Repository.
4	Set up the databases for audit, directing each database's audit information to its own Repository.
5	Set up separate SQL login accounts for the two databases.

## Prerequisites and installation

To ensure that the prerequisites for installation are met and to install Entegra software, do the following:

1. Ensure that all machines meet the hardware, software/operating system, and network connectivity requirements described in Chapter 2.
2. Ensure that login names and passwords are available that fit the criteria described in the "Security" section of Chapter 2. For the purpose of this example, use SQL authentication to connect to the two databases. You need a single SQL username and password that has sysadmin privileges on both databases on SERVER1.
3. Log on to ENTEGRA1 using a Windows login that has full administrative privileges on the machine.
4. Using the provided media, install the Entegra Management Console on ENTEGRA1.
5. Log on to ENTEGRA2 using a Windows login that has full administrative privileges on the machine.
6. Using the provided media, install the Entegra Web Server on ENTEGRA2.

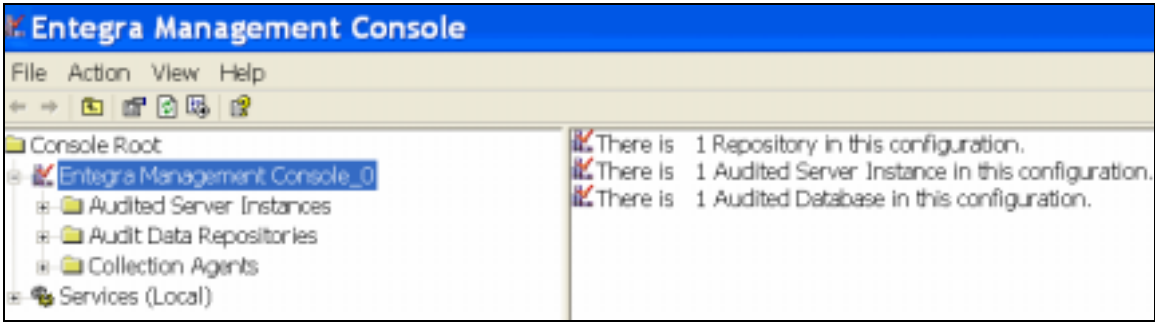
This concludes the installation portion of the setup process. Next, we set up SERVER1 as an Audited Server Instance, and deploy Agents.

## Add an Audited Server Instance and deploy Agents

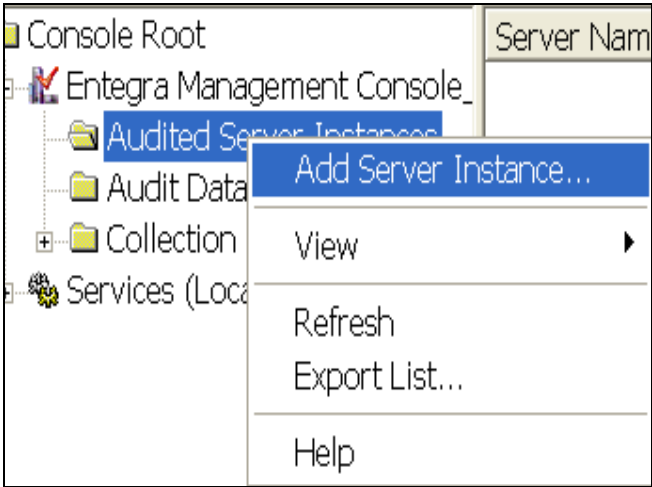
To add an Audited Server Instance, and deploy Agents, do the following:

1. On ENTEGRA1, launch the Management Console from the desktop shortcut or the Start Menu (*Start, Programs, Lumigent, Entegra, Management Console*).

The initial screen resembles the following:



2. Right-click **Audited Server Instances**, and then select **Add Server Instance**.





The “Add Server Instance to Audit” wizard is displayed.

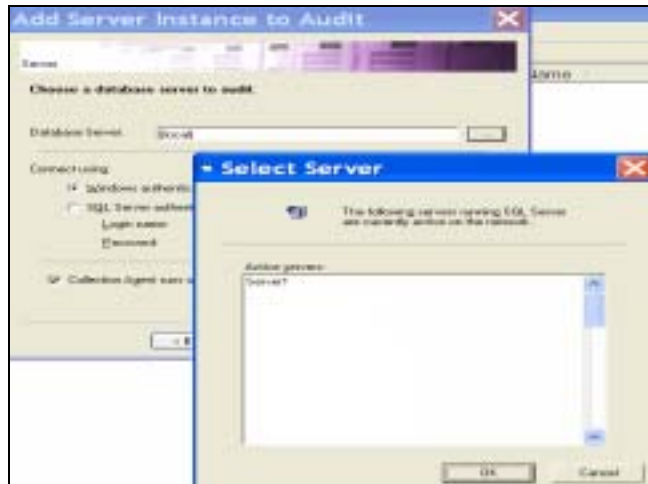


3. Click **Next**.

The screen where you choose a database server to audit is displayed.

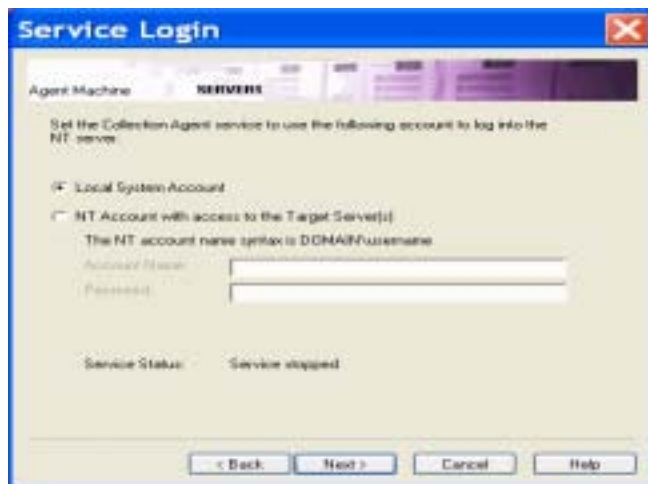


4. In the Database Server text box, type SERVER1, or click the browse button ... to display the available database servers as shown below. Select SERVER1, and then click **OK**.



5. Select the **SQL Server authentication** radio button and enter the username and password for a SQL account that has sysadmin privileges on SERVER1.
6. Make sure that the **Collection Agent runs on same machine** check box is selected, and click **Next**.

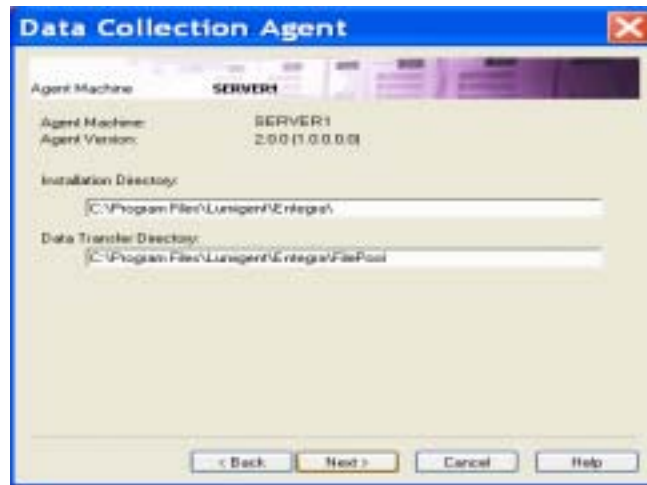
The "Service Login" screen is displayed.



This screen asks for login information that the Collection Agent uses to run its service. The local system account is the default. Alternatively, you can specify a username and password. This account must have "logon as service" permission on SERVER1.

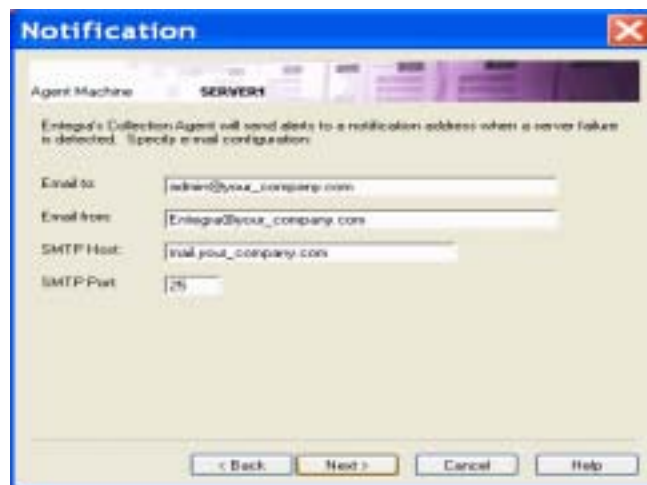
7. Click **Next**.

The “Data Collection Agent” screen is displayed.



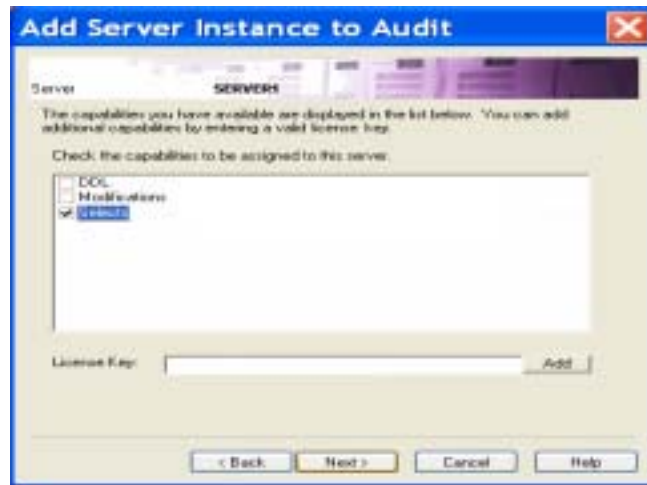
8. Select the locations where you want the Collection Agent installed and where you want it to store its audit data files, and then click **Next**.

The “Notification” screen is displayed.



9. Enter email information for the Collection Agent to use when emailing you about collection failures. You must enter a To and From email address, and the name of your mail server, and then click **Next**.

The screen where you select your licensed capabilities is displayed.



10. Type or paste the Entegra license key into the **License Key** text box and click **Add**.  
All Entegra features available in this key are displayed in the window.
11. Check the boxes next to the features that you wish to enable for this audited server instance, and then click **Next**.

The screen that allows you to set auditing frequency is displayed.



12. Set the schedule for automatic collection.

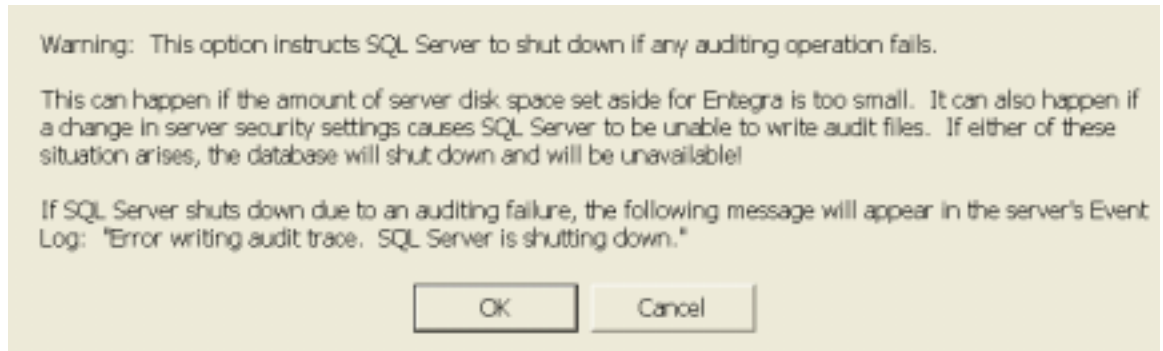
Recommendation: Schedule collections for low-traffic times of day. Also, avoid overlap of collection and backup operations. Ideally, collections should be run shortly after the backup completes.

For this example, set the collection schedule to 7:00 A.M and 7:00 P.M. every day. To do so, click the arrow:

- a. In the Start Date box, select tomorrow's date.
- b. In the Start Time box, select 7:00 A.M.
- c. In the Frequency section, change the units to "hours" and enter 12 in the text box.

13. To choose the option, **Shutdown the server on audit error to protect audit integrity**, select the check box, and then click **Next**.

Note: If you select this option, the following warning is displayed:



14. Click **OK** to accept this option, or click **Cancel** to clear it.

The screen that allows you to specify how alerts are sent from the server is displayed.



This optional feature alerts you any time an event of a specified type occurs. (You specify the types of events that trigger alerts in the next step.) By default, alerts are logged to the Windows Event Log on the local server.

15. Select the methods by which you want to be notified when an alert condition occurs. To have alert events emailed, select the **Email to:** check box, make any modifications in the text boxes, and then click **Next**.

The screen that allows you to select alert events is displayed.



16. Select database events that you wish to be alerted of in real-time, and then click **Next**.

**Important:** Selecting the **Successful login** option generates a large number of alerts. If these alerts are emailed to you, server performance may be impacted.

The screen that allows you to complete the configuration wizard is displayed.



17. Click **Finish** to complete the installation.

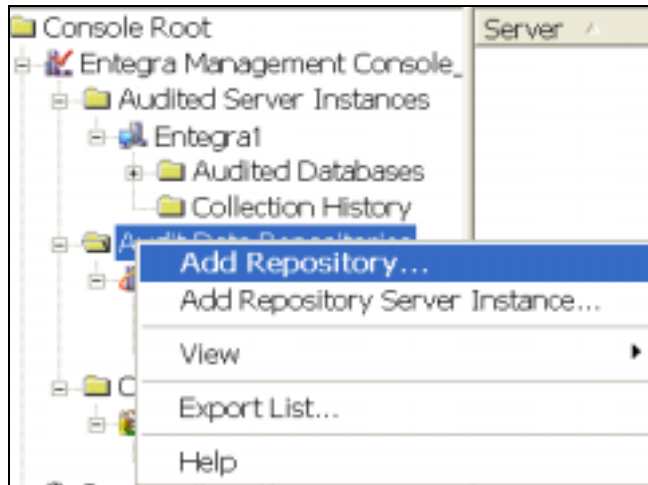
Entegra installs the Collection Agent and necessary components on SERVER1.

You have now finished setting up SERVER1 as an Audited Server Instance and deploying a Collection Agent. Next, create two Repositories to hold the audit data from the two databases you plan to audit.

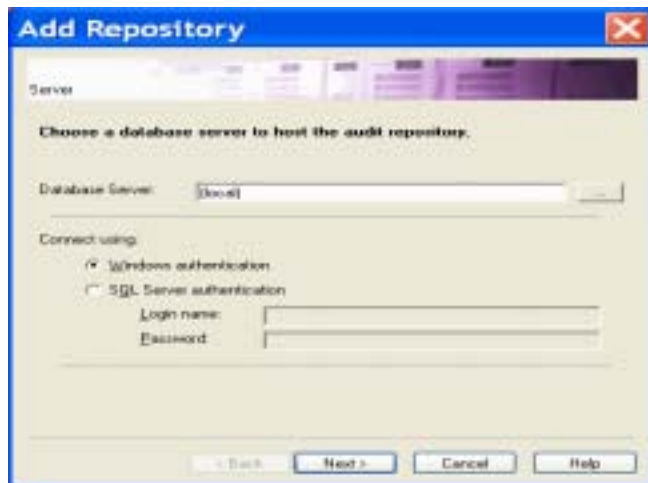
## Create a Payroll Repository

To create a payroll repository to hold the audit data from one of the two databases you plan to audit, do the following:

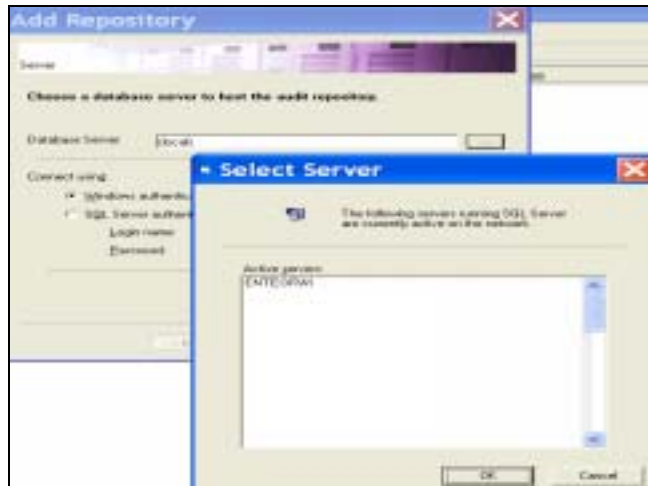
1. At the Entegra Management Console, right-click **Audit Data Repositories**, and then select **Add Repository**.



The “Add Repository” wizard is displayed.

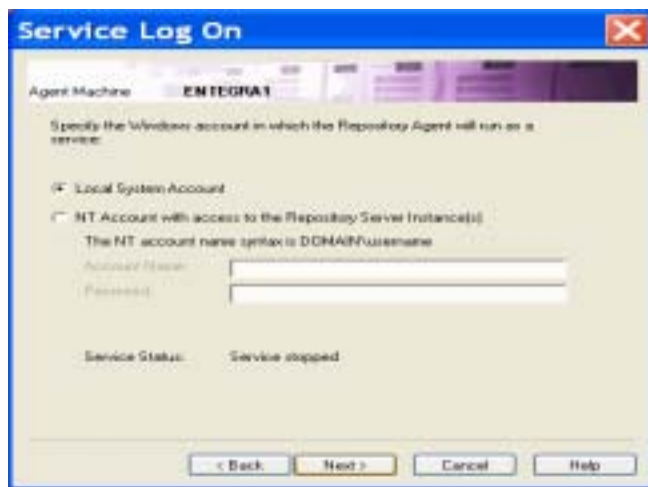


2. In the **Database Server** text box, type ENTEGRA1, or click the browse button **...** to display the available database servers as shown below. Select ENTEGRA1, and then click **OK**.



3. Select the **SQL server authentication** radio button, and enter the username and password for a SQL login account that has sysadmin privileges on ENTEGRA1, and then click **Next**.

The “Service Log On” screen is displayed.

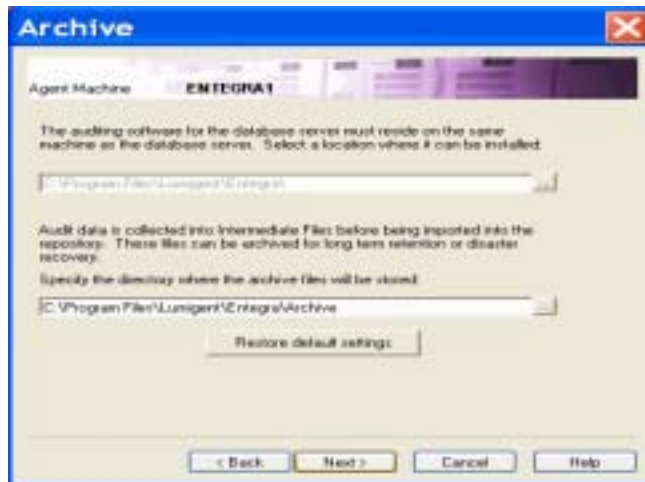


The Service Log On screen information is used by the Repository Agent to run its service.

4. Accept the Local System Account default, and then click **Next**.

The “Archive” screen is displayed.

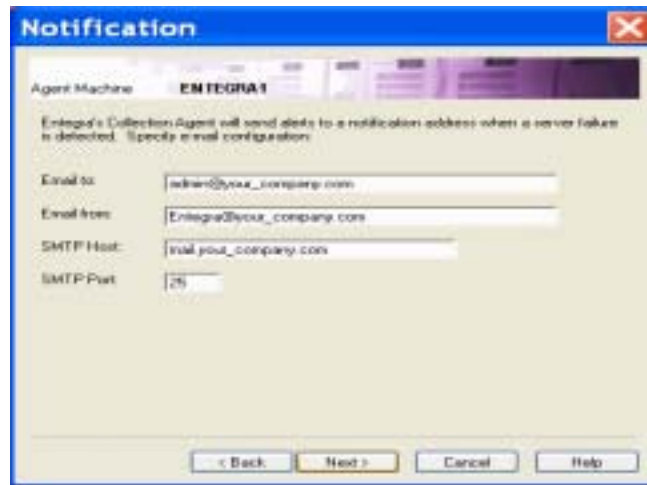




5. Select a location for audit data to be archived after it has been imported into the Repository, and then click **Next**.

For more details on this feature, see Chapter 4.

The “Notification” screen is displayed.

The "Notification" window has a blue title bar with the text "Notification" and a close button. Below the title bar is a header area with "Agent Machine" and "ENTEGRAT". The main content area contains the text: "Entegra's Collection Agent will send alerts to a notification address when a server failure is detected. Specify email configuration:". There are four text input fields: "Email to:" with the value "admin@your\_company.com", "Email from:" with the value "Entegra@your\_company.com", "SMTP Host:" with the value "mail.your\_company.com", and "SMTP Port:" with the value "25". At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

6. Enter email information for the Repository Agent to use when emailing you about import failures, and then click **Next**.

The “Add Repository” screen is displayed.

The "Add Repository" window has a blue title bar with the text "Add Repository" and a close button. Below the title bar is a header area with "Server" and "ENTEGRAT". The main content area contains the text: "Provide a name for the new Repository. This will be the name of the Repository you will see in the Entegra Browser user interface:". There is a text input field for "Repository Name:" with the value "Payroll\_Repository". Below this is the text: "Specify a database where the Repository will be created. More than one Repository can be kept in the same database. The amount of space required depends on the amount of data collected from the Database you are adding:". There is a dropdown menu for "Database:" with the value "lureagent". Below this is a text input field for "License Key:" and a button labeled "Add". At the bottom are four buttons: "< Back", "Finish", "Cancel", and "Help".

7. In the **Repository Name** text box, type **Payroll\_Repository**.
8. In the Database text box, type **payroll**.

Note that this screen also allows you to specify a Repository license key. If the license that you entered during the Add Audited Server Instance Wizard included Repository capabilities, it is displayed and can be used for the Repository you are now creating. If not, you must enter a valid Repository license key before continuing.


9. Click **Finish** to set up ENTEGRA1 as a Repository Server and create the new Repository.

## Create a Customer Repository

To create a customer repository to hold the audit data from one of the two databases you plan to audit, do the following:

1. At the EMC, expand the **Audit Data Repositories**, right-click ENTEGRA1, and select **Add Repository**.

The “Add Repository” screen is displayed.



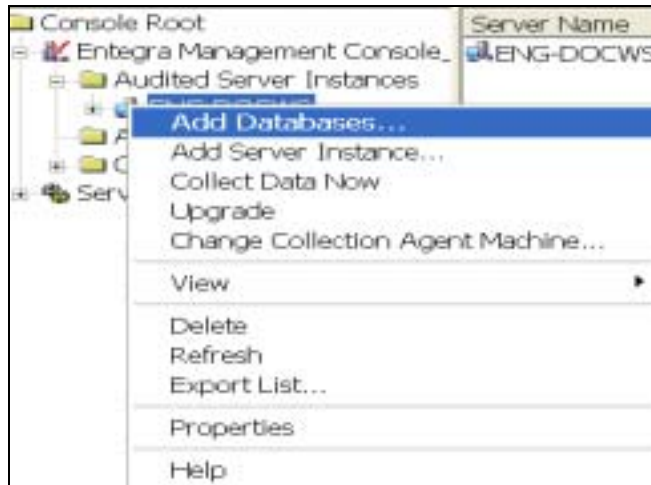
2. In the **Repository Name** text box, type **Customer\_Repository**.
3. In the **Database** text box, type **customer**.
4. Click **Finish** to create the repository.

You have finished creating the two Repositories and created tables in a database for each repository. Next, you set up the databases for audit, directing each database's audit information to its own Repository.

## Set up the databases for audit, directing each database's audit information to its own Repository


To set up the databases for audit, directing each database's audit information to its own Repository, do the following:

1. At the EMC, expand **Audited Server Instances**, right-click SERVER1, and then select **Add Databases**.



The “Add Databases to Audit” wizard is displayed.



2. Select the Payroll database (in this example, it is lumigent) from the **Available Databases** window, and click the right-arrow button  to move it to the **Target Databases** window, and then click **Next**.

Tip: You can also double-click databases to move them.

The screen with the databases that you selected to audit is displayed.

Note: Only newly selected databases are displayed; databases that are already set up for audit are not displayed.



3. Ensure that the **Enable Data Modification auditing on all tables** check box is selected and, if available, that the **Enable SELECTs auditing on all tables and views** check box is clear, and then click **Next**.

If you are certain that the backup log for the selected databases is not in the SQL Server default location, enter it in the **Backup log path** box; otherwise leave the default. (For a full explanation of the other options on this screen, see Chapter 4.)

The following screen is displayed.



4. Click the down arrow, select **Payroll\_Repository** from the drop-down menu, and then click **Next**.

The screen that allows you to complete the configuration wizard is displayed.



5. Verify that all your selections are correct, and click **Finish**.

The Payroll database is now set up for auditing.

6. Repeat the previous five steps for the Customer database and the Customer\_Repository.

You have finished the configuration process. Audit data from your databases is collected according to the schedule you selected.

To collect data immediately, right-click SERVER1, and then select **Collect Data Now**.

## Set up separate SQL login accounts for the two databases

For security purposes, you need to set up two separate SQL login accounts for the two databases. Do the following, using the same procedure as for ENTEGRA1:

1. On ENTEGRA2, use SQL Enterprise Manager to create two new accounts.
2. Create user account 'payroll' with read privileges on the Payroll\_Repository.
3. Create user account 'customers' with read privileges on the Customer\_Repository.
4. Optionally, you may also create a user account with read privileges on both Repositories.

Users can now view audit data by using the installed desktop shortcuts, or by connecting their browsers to `http://ENTEGRA1:8080/lumigent/login.html` and logging in with the appropriate permissions (see Chapter 6).

## Example 3: Variation of setting up three machines as an Entegra environment

In Example Three, there are three machines in our environment. Two existing SQL Server machines called SERVER1 and SERVER2 hold important databases:

- Payroll on SERVER1
- Customers on SERVER2

A third machine, ENTEGRA1, holds the Repository and Web Server.

In this setup, you install one Collection Agent on the Audited Server Instance SERVER1 for convenience. This Agent handles both SERVER1 and SERVER2. (On high-volume systems you can run the Collection Agent on a machine other than the Audited Server Instance, as shown in Example 1. The Collection Agent may cause slight performance degradation on a server machine.)

This example takes you through the following stages:

Stage	What Happens
1	Prerequisites and installation.
2	Add the first Audited Server Instance and deploy Agents.
3	Add the second Audited Server Instance and deploy Agents.
4	Create a Repository to hold the audit data from the two databases you plan to audit.
5	Set up the databases for audit.

## Prerequisites and installation

To ensure that the prerequisites for installation are met and to install Entegra software, do the following:

1. Ensure that all machines meet the hardware, software/operating system, and network connectivity requirements described in Chapter 2.
2. Ensure that login names and passwords are available that fit the criteria described in the "Security" section of Chapter 2.

For the purpose of this example, use Windows authentication to connect to the databases on both servers. You need Windows usernames and passwords that have sysadmin privileges on the servers.

3. Log on to ENTEGRA1 using a Windows login that has full administrative privileges on the machine.
4. Using the provided media, install the Entegra Management Console and Web Server on ENTEGRA1.

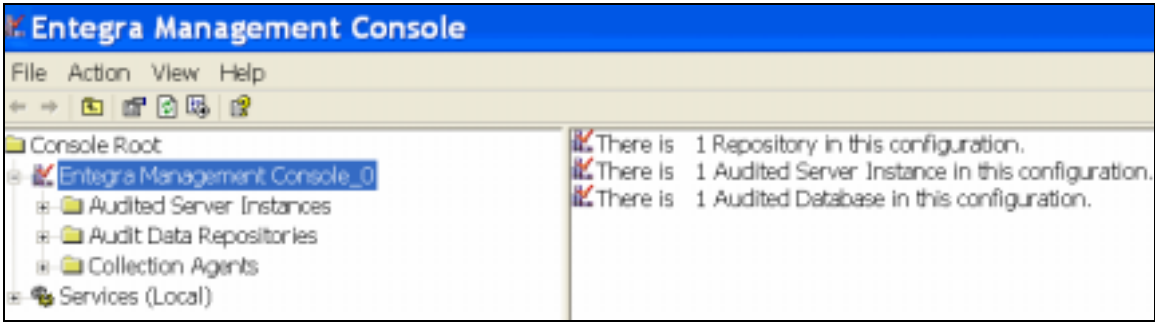
This concludes the installation stage of the setup process. Next, you set up SERVER1 and SERVER2 as an Audited Server Instance, and deploy the Collection Agent.

## Add the First Audited Server Instance, and deploy Agents

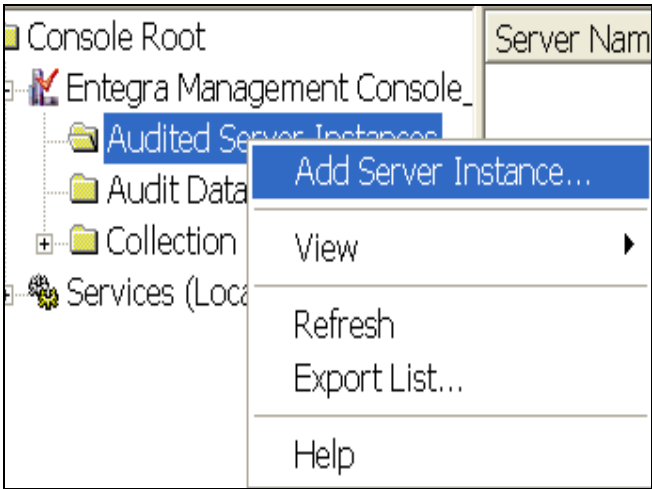
To add the first Audited Server Instance, and deploy Agents, do the following:

1. Launch the Management Console from the desktop shortcut or the Start Menu (*Start, Programs, Lumigent, Entegra, Management Console*).

The Entegra Management Console screen resembles the following:



2. Right-click **Audited Server Instances**, and then select **Add Server Instance**.



The “Add Server Instance to Audit” wizard is displayed.



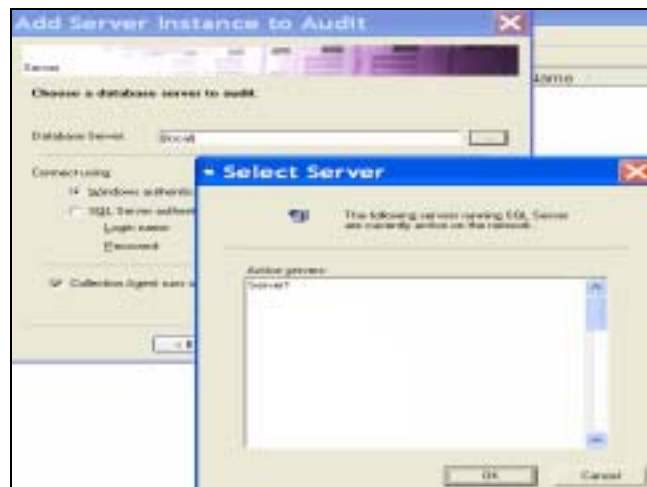
3. Click **Next**.



The screen where you choose a database server to audit is displayed.

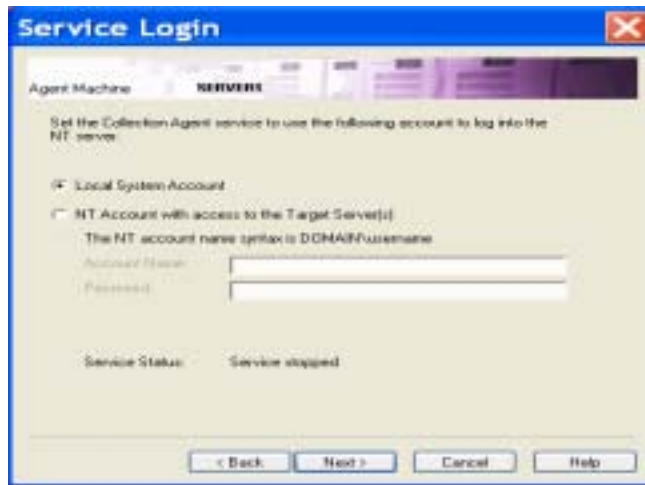


4. In the **Database Server** text box, type SERVER1, or click the browse button ... to display the available database servers as shown below. Select SERVER1, and then click **OK**.



5. Accept the default Windows authentication, make sure that the **Collection Agent runs on same machine** check box is selected, and then click **Next**.

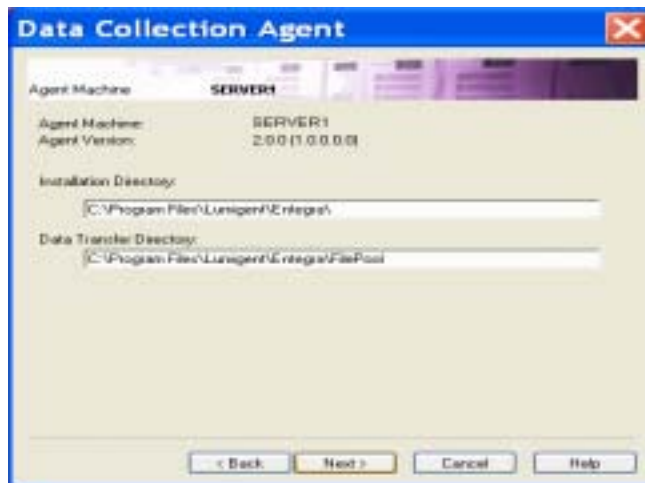
The “Service Login” screen is displayed.



This screen asks for login information that the Collection Agent uses to run its service. The local system account is the default. However, because this agent is managing an audited server on a separate machine, specify a username and password. This account must have "logon as service" permission on SERVER1.

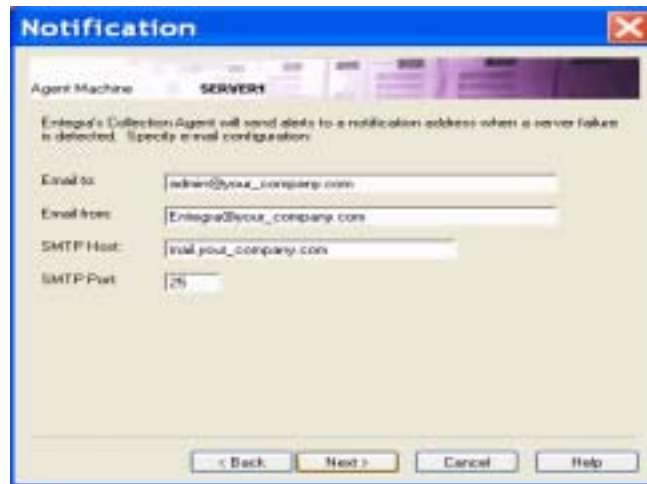
6. Specify a Windows login, and then click **Next**.

The “Data Collection Agent” screen is displayed.



7. Select the locations where you want the Collection Agent installed and where you want it to store its audit data files, and then click **Next**.

The “Notification” screen is displayed.

The "Notification" window has a blue title bar with the text "Notification" and a close button. Below the title bar is a tabbed interface with "SERVER1" selected. The main area contains the text: "Entegra's Collection Agent will send alerts to a notification address when a server failure is detected. Specify email configuration:". There are four text input fields: "Email to:" with "admin@your\_company.com", "Email from:" with "Entegra@your\_company.com", "SMTP Host:" with "mail.your\_company.com", and "SMTP Port:" with "25". At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

8. Enter email information for the Collection Agent to use when emailing you about collection failures. You must enter a To and From email address, and the name of your mail server, and then click **Next**.

The screen that allows you to select your license capabilities is displayed.

The "Add Server Instance to Audit" window has a blue title bar with the text "Add Server Instance to Audit" and a close button. Below the title bar is a tabbed interface with "SERVER1" selected. The main area contains the text: "The capabilities you have available are displayed in the list below. You can add additional capabilities by entering a valid license key." and "Check the capabilities to be assigned to this server:". There is a list box with two items: "DDL" and "Modifications", with "Modifications" selected. Below the list box is a "License Key:" label and a text input field. To the right of the input field is an "Add" button. At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

9. Type or paste the license key into the **License Key** text box and click **Add**.  
All Entegra features available in this key are displayed in the Available Capabilities window.
10. Check the boxes next to the features that you wish to enable for SERVER1, and then click **Next**.

The screen that allows you to set auditing frequency is displayed.



11. Set the schedule for automatic collection.

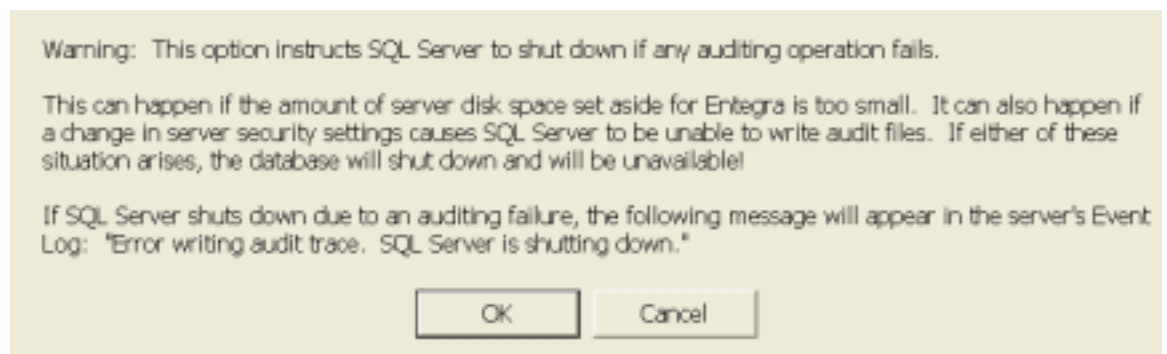
Recommendation: Schedule collections for low-traffic times of day. Also, avoid overlap of collection and backup operations. Ideally, collections should be run shortly after the backup completes.

For this example, set the collection schedule to 7:00 A.M and 7:00 P.M. every day. To do so, click the arrow:

- a. In the Start Date box, select tomorrow's date.
- b. In the Start Time box, select 7:00 A.M.
- c. In the Frequency section, change the units to "hours" and enter 12 in the text box.

12. To choose the option, **Shutdown the server on audit error to protect audit integrity**, select the check box, and then click **Next**.

Note: If you select this option, the following warning is displayed:



13. Click **OK** to accept this option, or click **Cancel** to clear it.

The screen that allows you to specify how alerts are sent from the server is displayed.

The screenshot shows the 'Add Server Instance to Audit' dialog box with the title bar in blue. The main area has a light yellow background. At the top, it says 'Server: SERVER1'. Below that, a text box explains: 'Specify how alerts will be sent from this server. The next page will let you select which events generate alerts. If you do not want any alerts generated, clear both the email and event log check boxes.' There are two checked checkboxes: 'Add alert events to the event log on this server' and 'Email to:'. The 'Email to:' section includes text boxes for 'Email to:' (containing 'Lunagard@lunagard.com'), 'Email from:' (containing 'Lunagard@lunagard.com'), 'SMTP Host:' (containing 'mail.lunagard.com'), and 'SMTP Port:' (containing '25'). At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

This optional feature alerts you any time an event of a specified type occurs. (You specify the types of events that trigger alerts in the next step.) By default, alerts are logged to the Windows Event Log on the local server.

14. Select the methods by which you want to be notified when an alert condition occurs. To have alert events emailed, select the **Email to:** check box, make any modifications in the text boxes, and then click **Next**.

The screen that allows you to select alert events is displayed.

The screenshot shows the 'Add Server Instance to Audit' dialog box with the title bar in blue. The main area has a light yellow background. At the top, it says 'Server: SERVER1'. Below that, a text box explains: 'An alert will be generated each time a selected event occurs in an audited database on server SERVER1.' There are several checked checkboxes: 'Create, Drop Database', 'Create, Alter, Drop Objects other than databases', 'Grant, Deny, Revoke Permissions', 'Add, Remove Login', 'Add, Remove User', 'Add, Remove Role', 'Restore Database', 'Failed login', and 'Successful login'. There are also unchecked checkboxes: 'Include Create, Alter, Drop of Temporary Tables', 'Database Console Command (DBCC)', 'Backup Database', and 'Logout'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

15. Select database events that you wish to be alerted of in real-time, and then click **Next**.

Important: Selecting the **Successful login** option generates a large number of alerts. If these alerts are emailed to you, server performance may be impacted.

The screen that allows you to complete the configuration wizard is displayed.



16. Click **Finish** to complete the installation.

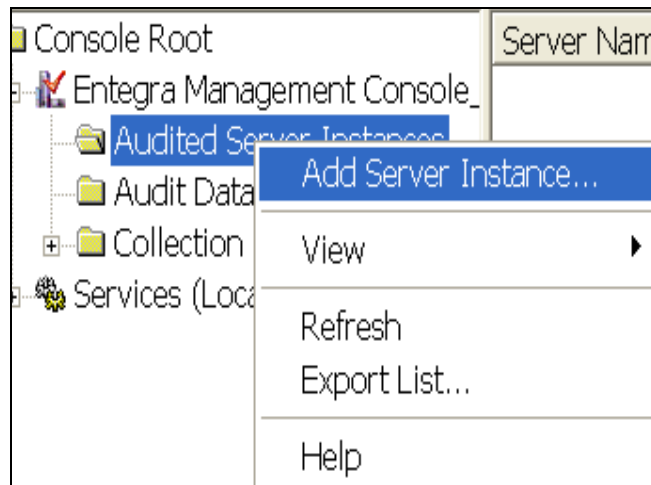
Entegra installs the Collection Agent and necessary components on SERVER1.

You have now finished setting up SERVER1 as an Audited Server Instance and deploying Agents.

## Add the second Audited Server Instance and deploy Agents

To add the second Audited Server Instance and deploy Agents, do the following:

1. Right-click **Audited Server Instances**, and then select **Add Server Instance**.



The “Add Server Instance to Audit” wizard is displayed.



2. Click **Next**.

The screen where you choose a database server to audit is displayed.



3. In the **Database Server** text box, type SERVER2, or click the browse button ... to display the available database servers. Select SERVER2, and then click **OK**.
4. Select the **SQL Server authentication** radio button, type a login name and password, clear the **Collection Agent runs on same machine** check box, and then click **Next**.

The screen that allows you to add a machine for the collection agent is displayed.



5. In the **Agent Machine** text box, type SERVER1, and then click **Next**.

The screen that allows you to select your license capabilities is displayed.



6. Type or paste the license key into the **License Key** text box and click **Add**.  
All Entegra features available in this key are displayed in the window.
7. Check the boxes next to the features that you wish to enable for this audited server instance, and then click **Next**.



The screen that allows you to set auditing frequency is displayed.



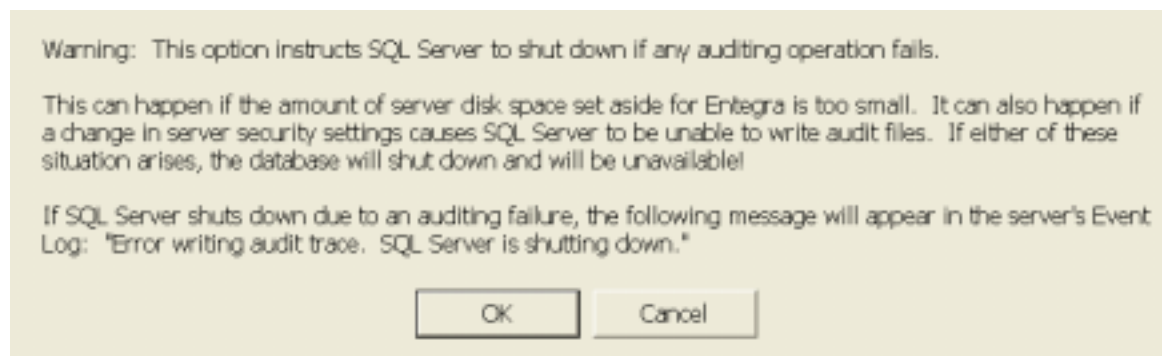
8. Set the schedule for automatic collection.

Recommendation: Schedule collections for low-traffic times of day. Also, avoid overlap of collection and backup operations. Ideally, collections should be run shortly after the backup completes.

For this example, set the collection schedule to 7:00 A.M and 7:00 P.M. every day. To do so, click the arrow:

- a. In the Start Date box, select tomorrow's date.
  - b. In the Start Time box, select 7:00 A.M.
  - c. In the Frequency section, change the units to "hours" and enter 12 in the text box.
9. To choose the option, **Shutdown the server on audit error to protect audit integrity**, select the check box, and then click **Next**.

Note: If you select this option, the following warning is displayed:



10. Click **OK** to accept this option, or click **Cancel** to clear it.

The screen that allows you to specify how alerts are sent from the server is displayed.

The screenshot shows a dialog box titled "Add Server Instance to Audit" with a close button (X) in the top right corner. The "Server" field is set to "SERVER2". Below this, a text box explains: "Specify how alerts will be sent from this server. The next page will let you select which events generate alerts. If you do not want any alerts generated, clear both the email and event log check boxes." There are two checked checkboxes: ☒ "Add alert events to the event log on this server" and ☐ "Email to:". The "Email to:" section includes text boxes for "Email to:" (containing "Lunaport@lunaport.com"), "Email from:" (containing "Lunaport@lunaport.com"), "SMTP Host:" (containing "mail.lunaport.com"), and "SMTP Port:" (containing "25"). At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

This optional feature alerts you any time an event of a specified type occurs. (You specify the types of events that trigger alerts in the next step.) By default, alerts are logged to the Windows Event Log on the local server.

11. Select the methods by which you want to be notified when an alert condition occurs. To have alert events emailed, select the **Email to:** check box, make any modifications in the text boxes, and then click **Next**.

The screen that allows you to select alert events is displayed.

The screenshot shows the same dialog box, but now it's at the step where you select alert events. The "Server" field is still "SERVER2". A text box explains: "An alert will be generated each time a selected event occurs in an audited database on server SERVER2." There are several checked checkboxes: ☒ "Create, Drop Database", ☒ "Create, Alter, Drop Objects other than databases" (with an unchecked sub-option "Include Create, Alter, Drop of Temporary Tables"), ☒ "Grant, Deny, Revoke Permissions", ☒ "Add, Remove Login", ☒ "Add, Remove User", ☒ "Add, Remove Role", ☐ "Database Console Command (DBCC)", ☒ "Restore Database" (with an unchecked sub-option "Backup Database"), ☒ "Failed login" (with unchecked sub-options "Successful login" and "Logout"). At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

12. Select database events that you wish to be alerted of in real-time, and then click **Next**.

Important: Selecting the **Successful login** option generates a large number of alerts. If these alerts are emailed to you, server performance may be impacted.

The screen that allows you to complete the configuration wizard is displayed.



13. Click **Finish** to complete the installation.

Entegra installs necessary components on SERVER2 and adds the SERVER2 setup information to the configuration of the Collection Agent on SERVER1.

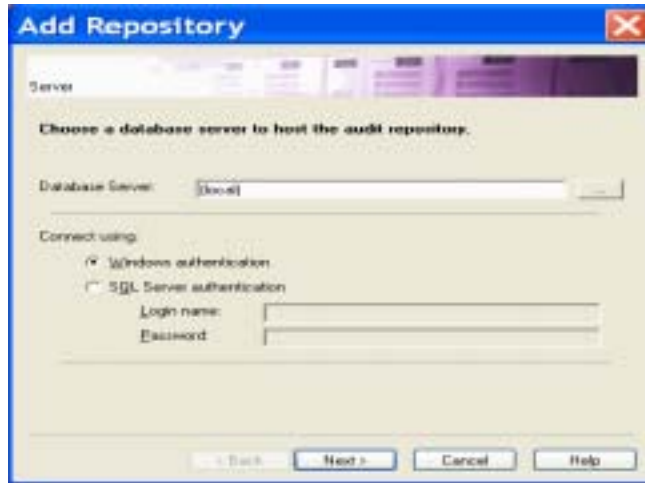
You have now finished setting up your two servers as Audited Server Instances and deploying Collection Agents. Next, you create a Repository to hold the audit data from the two databases you plan to audit.

## Create a Repository to hold the audit data from the two databases you plan to audit

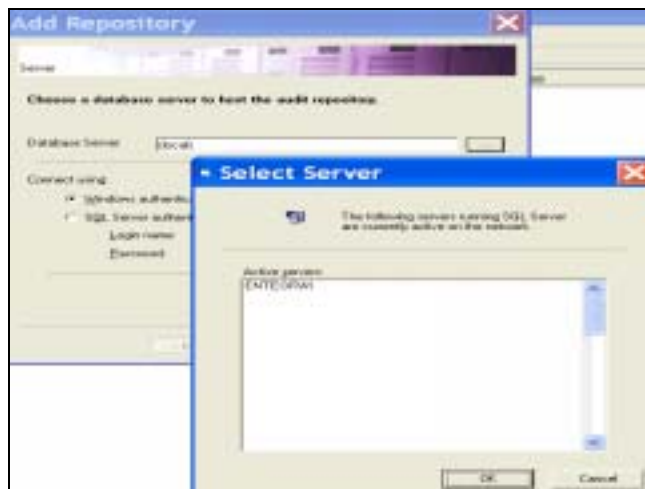
To create a Repository to hold the audit data from the two databases you plan to audit, do the following:

1. At the Entegra Management Console, right-click **Audit Data Repositories**, and then select **Add Repository**.

The “Add Repository” wizard is displayed.

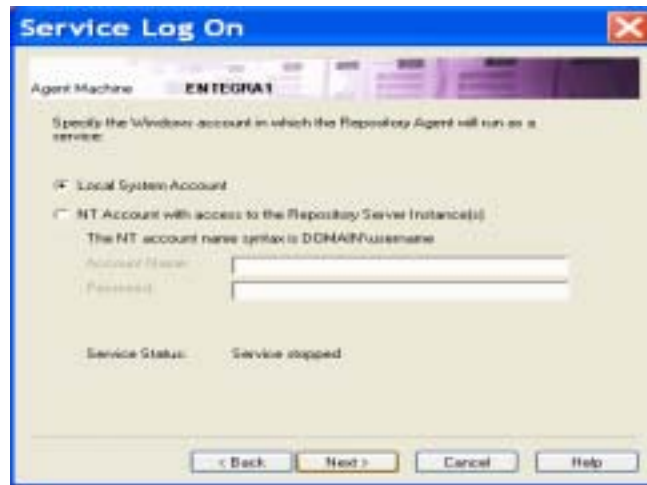


2. In the **Database Server** text box, type ENTEGRA1, or click the browse button ... to display the available database servers as shown below. Select ENTEGRA1, and then click **OK**.



3. Select the **SQL Server authentication** radio button, and enter the username and password for a SQL login account that has sysadmin privileges on ENTEGRA1, and then click **Next**.

The “Service Log On” screen is displayed.

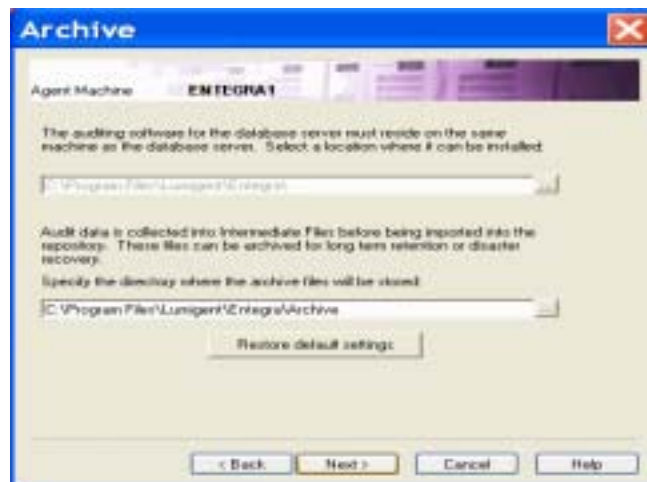


The Service Log On screen information is used by the Repository Agent to run its service.

4. To use the local system account, accept the Local System Account default, and then click **Next**. Alternatively, you can specify a username and password.

This account must have "logon as service" permission on ENTEGRA1.

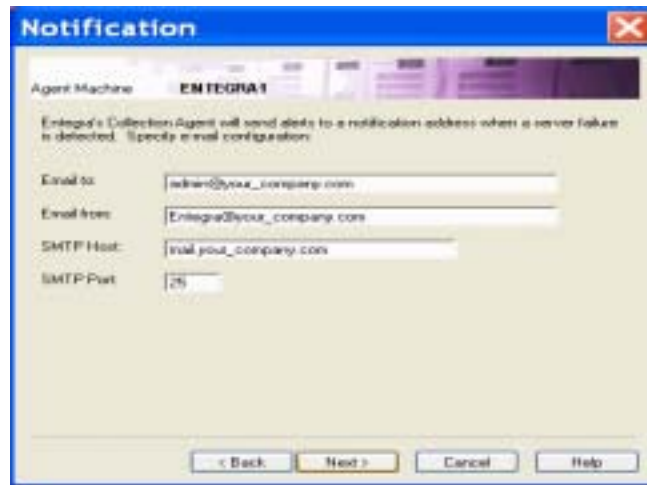
The “Archive” screen is displayed.



5. Select a location for audit data to be archived after it has been imported into the Repository, and then click **Next**.

For more details on this feature, see Chapter 4.

The “Notification” screen is displayed.

The screenshot shows a window titled "Notification" with a blue header bar. Below the header, there's a section for "Agent Machine" labeled "ENTEGRA1". A message states: "Entegra's Collection Agent will send alerts to a notification address when a server failure is detected. Specify email configuration:". There are four input fields: "Email to:" with the value "admin@your\_company.com", "Email from:" with "Entegra@your\_company.com", "SMTP Host:" with "mail.your\_company.com", and "SMTP Port:" with "25". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

6. Enter email information for the Repository Agent to use when emailing you about import failures, and then click **Next**.

The “Repository Database” screen is displayed.

The screenshot shows a window titled "Repository Database" with a blue header bar. Below the header, there's a section for "Server" labeled "ENTEGRA1". A message states: "Provide a name for the new Repository. This will be the name of the Repository you will see in the Entegra Browser user interface:". There is an input field for "Repository Name:" with the value "Default\_Repository\_1". Another message states: "Specify a database where the Repository will be created. More than one Repository can be kept in the same database. The amount of space required depends on the amount of data collected from the Database(s) you are auditing." There are two dropdown menus: "Database:" with the value "lumigent" and "Product Key:" which is empty. An "Add" button is next to the Product Key field. At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

7. Specify a name for the new Repository, and then click **Next**.

By default, the repository is named "Default\_Repository." You can also select an alternate database for the Repository to reside in. By default, it is installed in the lumigent database.

Restriction: Using a non-alphanumeric character as the first character of a repository name can cause problems. Use an alphanumeric character to begin a repository name. You may use special characters (the following are accepted: @ \_ \$ #) elsewhere in the repository name.

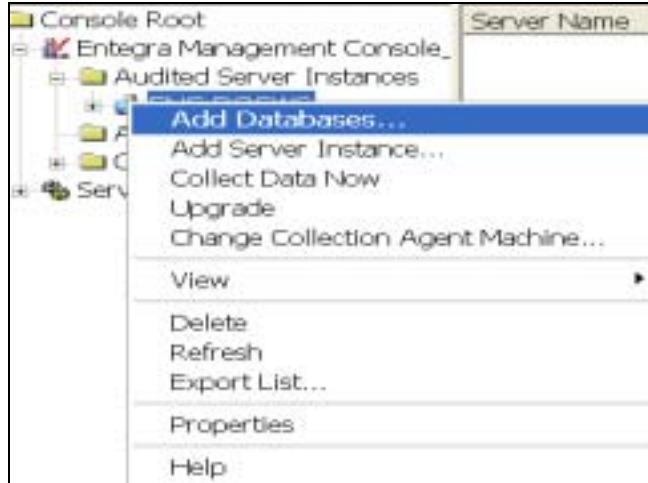
8. Click Finish to set up ENTEGRA1 as a Repository Server and create the new Repository.

You have finished setting up the Repository Server and creating the Repository. Next, set up the databases for audit.

## Set up the databases for audit


To set up the databases for audit, do the following:

1. At the EMC, expand **Audited Server Instances**, right-click SERVER1, and then select **Add Databases**.



The “Add Databases to Audit” wizard is displayed.



2. Select the Payroll database (in this example, it is lumigent) from the **Available Databases** window, and click the right-arrow button  to move it to the **Target Databases** window, and then click **Next**.

Tip: You can also double-click databases to move them.

The screen with the database that you selected to audit is displayed.

Note: Only newly selected databases are displayed; databases that are already set up for audit are not displayed.



3. Ensure that the **Enable Data Modification auditing on all tables** check box is selected and, if available, that the **Enable SELECTs auditing on all tables and views** check box is clear, and then click **Next**.

If you are certain that the backup log for the selected databases is not in the SQL Server default location, enter it in the **Backup log path** box; otherwise leave the default. (For a full explanation of the other options on this screen, see Chapter 4.)

The following screen is displayed.



4. Click the down arrow, select a repository from the drop-down menu, and then click **Next**.



The screen that allows you to complete the configuration wizard is displayed.



5. Verify that your selections are correct, and click **Finish**.

The database is now set up for auditing.

6. Repeat the previous five steps, replacing SERVER1 with SERVER2 and the Payroll database with the Customer database.

You have finished the configuration process. Audit data from your databases is collected according to the schedule you selected.

7. If you wish to collect data immediately, expand **Audited Server Instances**, right-click a server name and select **Collect Data Now**.

Users can now view audit data by using the installed desktop shortcuts, or by connecting their browsers to `http://ENTEOPRA1:8080/lumigent/login.html` and logging in with the appropriate permissions (see Chapter 6).

## Example 4: The SQL Server instance being audited is part of a cluster

In Example 4, the SQL Server instance being audited is part of a cluster. This example assumes that the Audited Server Instance resides on the active node of an active/passive cluster. All other components – the Entegra Management Console, Collection Agent, Repository, Repository Agent, and Web Server – reside on a separate machine outside the cluster.

This configuration is exactly the same as Example 1. In this case “SERVER1” would be the server instance name of a clustered server. The collection agent and repository are on a non-clustered machine, ENTEOPRA1. This is the recommended configuration when auditing a clustered server.

(Note that the Management Console and Web Server may be installed on cluster machines as well if desired. The Collection Agent, Repository, and Repository Agent are the only components that must *not* be installed on a cluster.)



---

# Chapter 4: Archiving

The archiving feature provides an added layer of security for your databases in the case of data loss due to hardware or software failure, or user error. With archiving enabled, all Intermediate Files are retained on the Repository machine indefinitely.

## Archiving Process

After audit data is collected by the Collection Agent, the archiving process is as follows:

Stage	What Happens
1	The audit data is packaged into an Intermediate File.
2	The Intermediate File is sent to the Repository Agent on the Repository machine.
3	The Repository Agent extracts the audit data and uses it to populate the Repository.
4	The Intermediate File is then moved to an archive directory for storage.
5	Audit data in the Repository may be deleted after a certain amount of time has passed.

## Specifying Archive Options

There are three main options you can specify for the archiving feature:

- how the SQL backup log is handled after Entegra has finished processing it
- how the Entegra Intermediate File is handled after the data it contains has been imported into the Repository
- how long data is retained in the Repository before being purged

## SQL Backup Log Handling

At the **Add Database to Audit** wizard screen, you can specify the disk location of the SQL backup logs.

The same wizard screen also displays the **Post Processing** menu, which allows you to specify how Entegra handles the backup logs after audit data is extracted from them.

The following options are available:

- Leave the log in the backup directory
- Rename the log to a post processing directory
- Delete the log

### Leave the log in the backup directory

This option tells Entegra to do nothing after it is finished with the log. The log file remains in its directory indefinitely (or until you delete it, either manually or via another application).

### Rename the log to a post processing directory

This option tells Entegra to move the log to a separate directory after processing. If you select this option, the **Post Processing Directory** text box is displayed allowing you to select the directory to contain processed log files.

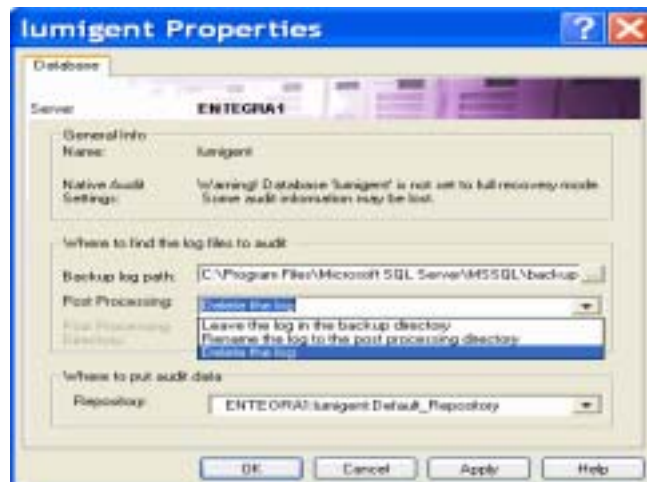
### Delete the log

This option tells Entegra to delete the log file from the disk after processing it. You can also view and change this setting after a database has been set up for auditing.

To delete the log, do the following:

1. Right-click the database name and select **Properties**.

The “Properties” screen is displayed.



2. At the **Post Processing** text box, click the down arrow, select **Delete the Log**, and then click **OK**.

## Entegra Intermediate File Handling

After you create a Repository, you can specify the directory in which Intermediate Files are stored on the Repository machine.

After Intermediate File data has been imported into the Repository, you are free to move it offline for storage purposes. For example, you can copy the files to tape backup or onto a CD-ROM to free hard drive space. Audit data may be purged from the Repository after a certain amount of time (see next section), so you need access to your Intermediate Files to restore this data.

To determine which Intermediate Files have been processed and can be safely removed from the disk, use SQL Server's Query Analyzer (or other query tool) to query the lumigent database on the Repository Server Instance.

Within lumigent, run the following query:

```
select status, pushfilename from lumAuditRepHistory
```

A status of 7 or 8 indicates that the file has been processed and can be removed from the archive directory. The pushfilename column displays the name of the Intermediate File.

After the intermediate files are permanently deleted, you are not able to restore or report on older audit data if that data is purged from the repository – unless you start over by deleting the repository and the database from audit, then adding them back into the audit.

## Purging Repository Audit Data

Audit data in the Repository may be purged after a certain amount of time has passed. You can specify this interval at setup time, or at any time thereafter, from the Entegra Management Console. By default, audit data is retained in the Repository indefinitely, but if you have a large amount of data, regularly purging the Repository has the following advantages:

- It speeds up import times
- It speeds up the Web Browser UI and automated reporting
- It reduces the amount of data displayed in the Web Browser

If you change **Retain Data Online (in days)** to be non-zero, all data beyond the number of days you set is purged from the Repository during the next Import operation into that repository.

Purged audit data can be restored from backed-up Intermediate Files (see "Restoring Archived Data" later in this chapter).

## Purging Data Procedure

To regularly purge audit data, do the following:

1. Right-click the Repository name and select **Properties**.

The “Properties” screen is displayed.



The **Retain Data Online (in days)** value controls how long (in days) data is kept in the Repository.

By default, this value is set to zero (0), meaning that audited data is never deleted from the Repository.

2. Set the **Retain Data Online (in days)** value to a number greater than zero.

Audit data older than the specified number of days is deleted from the Repository. However, because the Intermediate File is archived, deleted data can be retrieved at any time.

## About Restoring Audit Data

If you need to restore audit data that has been purged from the Repository, you can do so by using Entegra’s LMRestore utility to create a new Repository with the older audit data.

You provide the time range and audited database information, and the Repository Agent determines which Intermediate Files it needs to restore the requested information.

It then creates a new Repository, on a server instance that you specify, and populates it with the requested data.

You can browse the new Repository with the Browser as normal.

Although archived Intermediate Files are stored on disk, they need not remain there while not in use. You can move them to a different machine; copy them to tape or CD-ROM backup; or back them up using any other method of your choosing. When you attempt to restore the data from Intermediate Files that have been moved, you are prompted to replace the necessary files in the archive directory.

## Restoring Purged Audit Data

At any time you can restore audit data that has been purged from the Repository, provided that you still have the Intermediate Files containing the desired data. Entegra includes a command-line tool called LMRestore for restoring old data.

**Restriction:** Restored data cannot be replaced in the original Repository. The restore utility requires you to create a new Repository to hold the restored data.

You can create the new Repository on the same server instance that hosts the original Repository, or on a separate server instance.

## Restoring Data Procedure

To use the LMRestore utility to restore data, do the following:

1. Open a command prompt window and navigate to your Entegra installation directory (C:\Program Files\Lumigent\Entegra by default).
2. Type `lmrestore /list` and the following required switches:
  - `/SrcRepServer` - the server that hosts the repository to restore
  - `/SrcRepDB` - the database that hosts the repository to restore
  - `/SrcRepName` - the repository suffix of the repository to restore
  - `/StartTime` - the start timestamp for the restoration timerange
  - `/EndTime` - the end timestamp for the restoration

This command causes LMRestore to list all Intermediate Files that are needed for the restore (based on the parameters you specified), along with information on which of those files are on disk and which are missing.

If any files are listed as missing, you must locate them in your archives and replace them in the Intermediate File directory (see the section on Intermediate File Handling above).

3. Ensure that all necessary files are in the correct directory before you perform the next step.
4. Return to the command-line window and type `lmrestore/restore` and the following required switches:
  - `/SrcRepServer` - the server that hosts the repository to restore
  - `/SrcRepDB` - the database that hosts the repository to restore
  - `/SrcRepName` - the repository suffix of the repository to restore
  - `/StartTime` - the start timestamp for the restoration timerange
  - `/EndTime` - the end timestamp for the restoration
  - `/DestServer` - the destination server to which data is restored
  - `/DestDB` - the destination database to which data is restored
  - `/DestLogin` - the login to the destination server
  - `/DestPwd` - the password to the destination server
  - `/DestRepName` - the destination repository suffix

Note: See the switch description table and the examples below for more details.

## Switch Description Table

The following table lists the available switches and their purposes.

Switch	Description
/SrcRepServer	Name of the server instance that contains the Repository whose data you wish to restore.
/SrcRepDB	Name of the database that contains the Repository whose data you wish to restore (always lumigent).
/SrcRepName	Name of the Repository whose data you wish to restore.
/StartTime	Beginning of the time range you wish to restore. You can specify the time in one of three ways: <ul style="list-style-type: none"><li>▪ YYYY-MM-DD</li><li>▪ YYYY-MM-DD hh:mm:ss</li><li>▪ YYYY-MM-DD hh:mm:ss.mmm</li></ul>
/EndTime	End of the time range.
/DestServer	Name of the server instance onto which you want to restore the data.
/DestDB	Name of the database in which you want to create the new repository.
/DestRepName	Name of the new repository.
/DestLogin	Login name for the server instance specified in destserver.
/DestPwd	Password for the specified login name.

## Example of the Imrestore /list Command

This is an example of the Imrestore /list command:

```
C: \Program Files\Lumigent\Entegra>Imrestore /list /SrcRepServer Server1
/SrcRepDB lumigent /SrcRepName OldRepository /StartTime 2002-03-16
/EndTime 2002-04-13
```

The following example message is displayed:

```
/-----
// Lumigent Entegra LMRestore restore repository utility/
/
// Copyright 1999-2003 Lumigent Technologies, Inc. All rights reserved./
/-----
/ Listing archive files:

Repository = SERVER1: lumigent: OldRepository
timerange = 2000-03-16 00:00:00.000 to 2002-04-13 00:00:00.000
-- Files present in the archive ----

C: \Program
Files\Lumigent\Entegra\Archive\SERVER1_OldRepository_2001_10_01_15_00_07.
tmp
```



```
C: \Program  
Files\Lumigent\Entegra\Archive\SERVER1_OldRepository_2001_10_01_15_10_07.  
tmp
```

```
C: \Program  
Files\Lumigent\Entegra\Archive\SERVER1_OldRepository_2002_10_01_15_20_07.  
tmp
```

## Example of the Imrestore /restore Command

The following example shows the command for restoring a Repository.

In this example, the audit data was originally stored in repository **OldRepository** on server instance SERVER1. The restored data is stored in repository **NewRepository** on server instance SERVER2.

```
C: \Program Files\Lumigent\Entegra>Imrestore /Restore /SrcRepServer  
Server1 /SrcRepDB Lumigent /SrcRepName OldRepository /StartTime 2002-03-  
16 /EndTime 2002-04-13 /DestServer Server2 /DestDB Lumigent /DestRepName  
NewRepository /DestLogin sa /DestPwd server2password
```

The following example message is displayed:

```
/-----  
// Lumigent Entegra LMRestore restore repository utility.  
// Copyright 1999-2003 Lumigent Technologies, Inc. All rights reserved  
//-----  
-/ Restoring archive files:  
  
Repository = Server1: Lumigent: OldRepository  
timerange = 2002-03-16 00:00:00.000 to 2002-04-13 00:00:00.000  
Destination Repository: Server2: Lumigent: NewRepository  
  
- Creating ghost repository  
- Checking archive file list  
- All archived data files are present  
- Restoring 3 archived data files  
- RESTORATION IN PROGRESS. Monitor restoration progress from the Import  
History view under the Server2 repository server.  
- LMRestore is exiting
```



---

# Chapter 5: Entegra Management Console Reference

The Entegra Management Console provides a range of functionality for configuring and managing your Entegra setup. This chapter contains a comprehensive reference for all the functions and controls of the Management Console.

## Navigation Tree

This chapter provides information on all the options available to you in the EMC Navigation Tree. They include:

- Entegra Management Console\_0
- Audited Server Instances
- Audit Data Repositories
- Collection Agents

## Entegra Management Console\_0

This node lists the following

- Audited Server Instances
- Audit Data Repositories
- Collection Agents

## Console-Level Options

By right-clicking **Entegra Management Console\_0**, you access the following options:

Option	What it does
Delete All Objects	deletes all audit information for the objects referenced in the console file including repositories, audited server instances, and collection agents. Note: The <b>No</b> option deletes all objects except for repositories.
Upgrade	initiates an upgrade of all objects referenced in the console file.
View	allows you to determine how items are displayed in the result view of the console. The Detail view is recommended.
Refresh	refreshes the display.
Export List	allows you to export a list of audited servers into a text file.
Properties	allows you to view and/or configure licensing information such as which features are licensed for the server and which additional features you may enable on this server.
Help	launches the Lumigent Entegra online Help.

## Audited Server Instances

This node lists all SQL Server instances that you have set up for auditing. Under each server name is an "Audited Databases" node, which lists all databases on that server that are selected for audit.

You can add a new server to audit by right-clicking **Audited Server Instances** (or on any server's name) and selecting **Add Server Instance**. This launches the Add Audited Server Instance wizard.

## Server-Level Options

By right-clicking an audited server's name, you access the following options:

Option	What it does
Add Databases	launches the Add Database wizard.
Add Server Instance	launches the Add Audited Server Instance wizard.
Collect Data Now	instructs the Collection Agent associated with this server to begin a collection task.
Upgrade	initiates an upgrade of the Collection Agent and any audited servers being handled by that agent.
Change Collection Agent Machine	allows you to change the machine on which the Collection Agent for this server instance resides.
Delete	causes the selected server instance to be removed from the list of Audited Server Instances.
Refresh	refreshes the display.
Properties	<p>allows you to view and/or configure the following options for the selected audited server:</p> <ul style="list-style-type: none"><li>▪ Notification method for real-time alerts</li><li>▪ Database events you want to be notified about in real-time</li><li>▪ Schedule by which collection tasks are performed</li><li>▪ Login method for the Management Console and Agents to access the server's databases</li><li>▪ Licensing information such as which features are licensed for the server and which additional features you may enable on this server</li><li>▪ Installation path where the Collection Agent for this server is installed (this information cannot be changed)</li><li>▪ Location where the Collection Agent stores its working files</li></ul>
Help	launches the Lumigent Entegra online Help.

In addition, under each server is the "Collection History" node.

Highlight **Collection History** to reveal, in the details pane, information about all collection tasks that have occurred on the server. For each collection, you can see the following:

- start time
- status
- LSNs that form the boundaries of the data gathered in that collection
- location and filename of the Intermediate File

If the Collection History display becomes too long, you can purge it by right-clicking **Collection History** in the navigation pane and selecting **Purge**.

This command causes the Entegra Management Console to purge the display of all collection tasks except the most recent. The data collected in these tasks is still available. The Purge operation does not remove any data. It only removes information about the time and status of past collections. After a purge, you are not able to retrieve the collection history lines that were displayed – except for the last collection status for each audited database.

## Database-Level Options

By right-clicking the name of an audited database, you access the following options:

Option	What it does
Add Databases	launches the Add Database wizard.
Add or Remove Tables	opens the Add Table dialog.
Add or Remove Views	opens the Add View dialog.
Delete	causes the selected database to be removed from the list of Audited Databases.
Refresh	refreshes the display.
Properties	allows you to configure and/or view the following options for the selected database: <ul style="list-style-type: none"> <li>General information about the database.</li> <li>Status as to whether all required Audit components are set up for the database.</li> <li>Location of the SQL backup files for this database.</li> <li>Handling of SQL backup files after they are processed (see Chapter 4).</li> <li>Name of the Repository in which this database's audit data is stored.</li> </ul>
Help	launches the Lumigent Entegra online Help.

When you highlight a database name in the Console's navigation pane, the details pane displays the following:

- a list of audited tables and views in that database
- the type of audit
- the number of columns being audited
- the total number of columns for each table

The asterisk “\*” in the table detail view represents all columns in the table. The asterisk is used to avoid looking up the actual number of columns being audited. So an asterisk “\*” in the **Columns being audited** column means all columns in that table are being audited.

## Table-Level Options

By right-clicking the name of an audited table, you can access the following options:

Option	What it does
Add or Remove Columns	opens the Audited Table property page that allows you to select which columns in the table you want to audit.
Delete	removes the selected tables from the list of Audited Tables.
Refresh	refreshes the display.
Properties	allows you to configure and/or view the following options for the selected database: <ul style="list-style-type: none"><li>▪ Logical keys for this table.</li><li>▪ Which columns in this table are audited.</li><li>▪ Which events/operations on this table are audited.</li></ul>
Help	launches the Lumigent Entegra online Help.

## Audit Data Repositories

This node lists all SQL Server instances that you have set up as Repository Server Instances. Under each server is a list of Repositories that exist on that server. (It is possible to have a Repository Server with no Repositories on it.)

You can right-click **Audit Data Repositories** and select **Add Repository** to launch the Repository Server wizard followed by the Repository wizard. To add a Repository Server without also creating a new Repository on that server, right-click **Audit Data Repositories** and select **Add Repository Server Instance**.

## Server-Level Options

By right-clicking the name of a Repository Server Instance, you can access the following options:

Option	What it does
Add Repository	launches the Add Repository wizard to create a new repository on this server instance.
Upgrade	initiates an upgrade of the Repository Server and associated Repository Agent.
Delete	causes the selected Repository Server Instance (and all Repositories on that instance) to be removed.
Refresh	refreshes the display.
Properties	<p>allows you to configure and/or view the following options for the selected Repository Server Instance:</p> <ul style="list-style-type: none"><li>▪ the login method and username/password for the Management Console and Repository Agent to use to log on to the databases on this server</li><li>▪ the location of the Repository Agent for this server (this information cannot be changed)</li><li>▪ TCP ports for the Repository Agent to listen for commands and data from other Entegra components</li><li>▪ Location of audit archive logs (see Chapter 4)</li><li>▪ Email information for notifying you when the Repository Agent fails to import audit data.</li></ul>
Help	launches the Lumigent Entegra online Help.

In addition, under the Audit Data Repositories node you there is a folder called Import History.

When you highlight the Import History folder in the navigation pane, history information about recent import operations is displayed in the details pane.



## Repository-Level Options

By right-clicking the name of a Repository, you can access the following options:

Option	What it does
Add Repository	launches the Add Repository wizard.
Upgrade	initiates an upgrade of the Repository Server and associated Repository Agent.
Delete	causes the selected Repository to be removed.
Refresh	refreshes the display.
Properties	allows you to: <ul style="list-style-type: none"><li>▪ view configuration information about the Repository such as its name, location, and license information</li><li>▪ view and modify information such as how long to retain Intermediate Files (IFs) and where to store them on the Repository machine</li></ul>
Help	launches the Lumigent Entegra online Help.

## Collection Agents

This node lists all Collection Agents that you have set up on your system.

By expanding the "Collection Agents" tree, you can see a list of computers (by machine name) that have Collection Agents on them. Expand any machine name to see a list of the audited servers being handled by that Collection Agent.

By right-clicking **Collection Agents**, you can select **Add Collection Agent** to create a new Collection Agent.

The Agent software components are installed on the computer you specify, but the new Agent is not associated with any Audited Server Instances.

To assign the new Agent to an Audited Server Instance, right-click the desired server in the **Audited Server Instances** node, and select **Change Collection Agent Machine**.

## Agent-Level Options

By right-clicking the name of a Collection Agent machine, you can access the following options:

Option	What it does
Upgrade	initiates an upgrade of the Collection Agent.
Delete	causes the selected Collection Agent to be removed.
Refresh	refreshes the display.
Properties	<p>allows you to configure and/or view the following options for the selected Collection Agent:</p> <ul style="list-style-type: none"><li>▪ Installation location of the Agent, and the directory where it stores its files while processing them</li><li>▪ Port information for the Agent to use when listening for communication from the Entegra Management Console</li><li>▪ Email information for notifying you when the Collection Agent fails to collect audit data</li></ul>
Help	launches the Lumigent Entegra online Help.

---

# Chapter 6: Using the Entegra Browser

This chapter explains how to access and use the Entegra Browser to view your audit data.

## Necessary Permissions

For users to log on to the Entegra Browser and view data in the Repository, they must have certain permissions on the SQL Server instance that houses the Repository.

### On the Lumigent Database

Users logging in via the Entegra Browser must have read-only access to the following tables in the Lumigent database:

- lumAuditRepConfigVars
- lumAuditRepRepositories
- lumAuditRepHistory

These tables store important configuration information about the repository.

### On the Repository Database

Users also need read-only access on the database that houses the Repository. If the Repository resides in the Lumigent database, you can ignore the previous section and give users read-only access on lumigent.

## Starting the Entegra Web Server

Before you can use the Entegra Browser to browse your Repository, you need to do the following:

1. Start the Entegra Web Server.
2. Check the Windows Services control panel to verify that the web server is running.

## Shortcuts

At any time, you can stop or start the Entegra Web Server by using shortcuts on the Start Menu.

To access the shortcuts, select *Start, Programs*, (if XP: *All Programs*), *Lumigent, Entegra, Start Web Server* or *Stop Web Server*.

## Logging On

To access the Browser, do the following:

1. Click the installed desktop shortcut, or open Internet Explorer 6.0 and navigate to `//machine-name: 8080/lumigent/login.html`  
where machine-name is the name of the machine running the Web Server.
2. At the login screen, provide the required valid SQL Server username and password in the corresponding boxes.

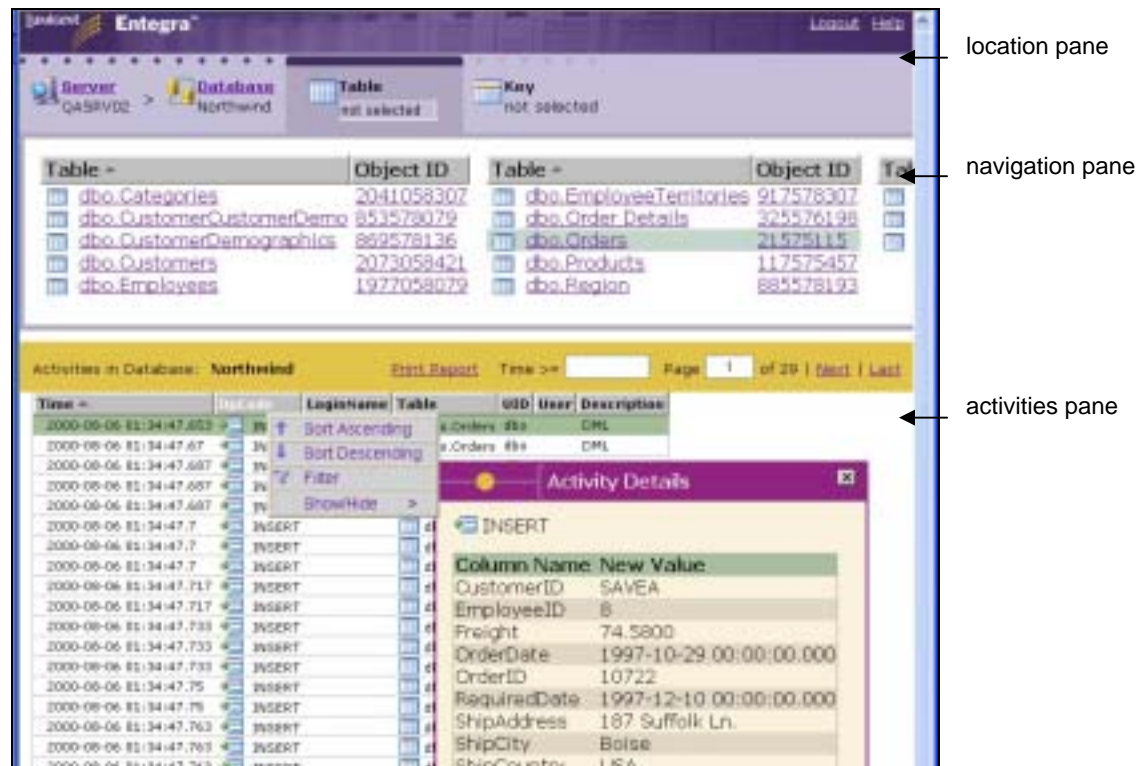
Requirements: You must use credentials that have the access rights described in the *Necessary Permissions* section.

You cannot use NT authentication to log on through the Entegra browser.

3. Type the server instance name in the Repository Server box (or select it from the drop-down menu), and click the **Get List of Repositories** button.  
A list of available Repositories on the selected server instance becomes available on the Repository drop-down menu.
4. Select the desired Repository and click the **Login to Repository** button.

# Viewing the Repository with the Entegra Browser

The Entegra Browser view consists of the following sections: the top navigation/location pane, which you can use to move around within the data and to narrow the selection of displayed data, and the bottom activities pane, which displays your actual audit data.



When you first log on to the Entegra Browser, all data for the selected Repository is displayed. The navigation pane shows the names of the Audited Server Instances whose audit data is contained in this Repository.

You can click an Audited Server Instance name to display a list of audited databases on that server; you can then click a database name to view a list of audited tables in that database.

Finally, you can click a table name to filter by logical keys. (After you have drilled down in the navigation pane, you can click **Table**, **Database**, or **Server** to return to the corresponding view.)

You can use the paging controls at the top right of the activities pane to move between pages of data. Initially, the word **multiple** is displayed in lieu of the total number of pages. To save time, Entegra does not automatically calculate the number of pages required. You can force calculation of the number of pages by clicking **multiple**.

Each row in the activities pane represents a single activity, with multiple columns of data about that activity. (For more detail on the activities pane, see the following sections.) When you highlight any row in the activities pane, the corresponding item in the navigation pane is highlighted.

For example, if the navigation pane is currently displaying a list of audited tables and you click a row in the activities pane that represents activity on the Customers table, that table is highlighted in the navigation pane. Similarly, clicking the Customers table in the navigation pane highlights all items in the activities pane that involve that table.

If you select a row in the view and it does not display a key in the status bar, it means that there are no logical keys selected for that table.

You may define the logical key in the EMC (See Selecting the Logical Key in Chapter 2). Collections from that point forward should have detailed activity recorded for that row and may be displayed in the transaction history.

The following sections provide more detail on sorting and filtering data.

## Sorting and Filtering Data

This section provides information on how to do the following:

- show/hide columns
- view details
- filter data

### Showing/Hiding Columns

To select the columns that are displayed in the activities pane, click any header, and then select **Show/Hide**.

To sort displayed data by a particular column, click the column header and select **Sort Ascending** or **Sort Descending**.

The following columns are displayed by default:

Column	What is displayed
LSN	The SQL Log Sequence Number of the transaction
Transaction ID	The SQL Transaction ID of the transaction
Time	The time the activity occurred
OpCode	Code indicating type of activity (SELECT, DELETE, INSERT, UPDATE)
LoginName	SQL Server login identifier of the user who initiated the activity
Table	The audited SQL table affected by the activity
Owner	The SQL user ID that initiated the activity
OS User	The Windows username that accessed the database to initiate the activity (in DOMAIN\user format)
Description	The type of activity (for example, DDL, DML, etc.)

The following columns are also available:

Column	What is displayed
Session ID	The SQL session ID in which the activity occurred
Activity ID	A unique ID assigned to the activity by Entegra
Client Hostname	Name of the machine from which the user was logged on
AppName	Name of the application that initiated the activity
Server	Name of the audited server on which the activity occurred
Database	Name of the database on which the activity occurred
Key	Concatenated values of the logical key columns for the affected row
Index	Internal-use column

## Filtering Data

The Entegra Browser provides several functions that allow you to filter data, thus narrowing the field so that you view only the data that interests you.

As described above, you can use the navigation pane to drill down and view data about a particular audited server, database, or table.

At the table level, you can click a table name in the navigation pane to access the Filter Keys dialog. This dialog allows you to enter a text string to be matched against the table's logical key. Entegra then displays that key value in the navigation pane; when you click it, rows whose key values match your selection are highlighted in the details pane.

A logical key can be typed in and/or selected from the view screen to get Row Revision History.

To filter on a particular column in the activities pane, click the column header and select **Filter**.

The resulting dialog allows you to select and display the specific values for this column.

## Viewing Details

For any activity row, you can view details about the activity by highlighting the row and clicking the **Show Details** link located at the lower right of the pane, or by double-clicking the row.

Depending on the type of activity involved, the Details window may show the exact SQL query that was entered, the old and new data (if the activity was an UPDATE statement), or other relevant data.

To see a complete history of changes affecting an individual row in an audited table, highlight a row in the Entegra Browser that corresponds to the audited database row in question, and then click the record key at the bottom of the Entegra Browser activities pane.

A yellow "caution" icon and the row's OpCode in red, indicates that the transaction failed.

If you cannot see the details for a particular field in the table, then use the EMC to add that column to the audit.

Changes to the configuration are not retroactive. If you start collecting new tables or columns, the data will be only for that collection forward. Entegra does not go back into old backup logs to get data if it already collected against that database.

If you never want to see the details for a particular field in the table, you can remove the table from the audit. Removing tables from the audit also saves resources and improves Entegra's performance. Refer to the Add/Remove Columns section for more detail.



---

# Chapter 7: Troubleshooting

This chapter discusses troubleshooting issues that you may encounter with your Entegra setup. If you get an unexpected error, contact [support@lumigent.com](mailto:support@lumigent.com). Attach the `emcerror.log` file from the Entegra installation directory. This file contains the error that was displayed. Support may also ask to see the application event logs from machines that are involved in the error you encountered.

## Entegra Management Console Issues

The following table lists EMC errors, a description of the error, and a recommended solution.

Error	Description	Recommendation
<b>Snap-In Failed To Initialize</b>	This error usually indicates that you are attempting to run the Entegra Management Console from a remote machine by opening the .msc file.	To solve the problem, run the Entegra installation program on the machine from which you want to use the Management Console.
<b>Transfer Failed</b>	<p>This message on the Collection History page can indicate a variety of problems with the following:</p> <ul style="list-style-type: none"> <li>▪ Collection Agent</li> <li>▪ Audited Server Instance</li> <li>▪ Repository Agent</li> </ul>	<p>To diagnose, check the Application Event Logs on the following:</p> <ul style="list-style-type: none"> <li>▪ the Collection Agent machine</li> <li>▪ the Audited Server Instance machine (if different)</li> <li>▪ the Repository machine (if different)</li> </ul> <p>Look for events from sources "LMExportAgent" or "LMExport." The text associated with the error event should provide further assistance.</p>
<b>Pinging sound or your machine stopped responding</b>	<p>On occasion, the EMC displays an error message, but the error message is hidden behind the main MMC window.</p> <p>Until the error message window is closed, the MMC makes a "ping" noise when clicked or your machine does not respond.</p>	<p>To display the error message, right-click the Windows task bar context menu and select <b>Tile Windows Horizontally</b> or <b>Tile Windows Vertically</b>.</p> <p>The error message window is displayed. Close the window to continue working.</p>
<b>Error message: Disabling E-mail Alerts on Server</b>	<p>The volume of alerts on the server ENTEGRA1-DESKTOP\SQL2000 is currently higher than the rate at which the e-mail server can process messages. Entegra is therefore temporarily disabling e-mail alerts on ENTEGRA1-DESKTOP\SQL2000. No more e-mail alerts will be sent until the frequency of alerts drops to a manageable level.</p> <p>This temporary change only affects e-mail alerts. Entegra is still gathering audit data. The audit trail in your Entegra repository is uninterrupted.</p>	<p>No corrective action is necessary. E-mail alerting will automatically resume once the frequency of alerts declines.</p> <p>If you receive this message often, you can reduce the number of e-mail alerts being sent by clearing some of the Alerts options.</p> <p>In the Entegra Management Console, right-click the Audited Server Instance ENTEGRA1-DESKTOP\SQL2000, select Properties, and click the Alerts tab.</p>

# Web Server and Browser Issues

This section describes common issues that may arise with the Entegra Web Server and/or Browser.

If you have tried all of the suggestions in the following sections and you are still having problems, please contact technical support as described in the preface to this book.

## Error Starting Web Server

If you are using Tomcat or another application, when starting the Entegra Web Server, you may observe the following error:

```
Catalina.start: LifecycleException: null.open: java.net.BindException:
Address in use: JVM_Bind: 8080
```

This error indicates that another application is using port 8080. As explained in Chapter 2, the Tomcat installation uses port 8080 by default.

To solve the problem, either identify the conflicting application and set it to use a different port, or change the Tomcat setup to a different port, as follows:

1. On the machine where you have installed the Entegra Web Server, navigate to `C:\Program Files\Lumigent\Entegra\WebUI\Server\conf` and open the `server.xml` file in a text editor.
2. Locate the following section of code:  

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8080" minProcessors="5" maxProcessors="75" enableLookups="true"
redirectPort="8443" acceptCount="10" debug="0"
connectionTimeout="20000" useURIValidationHack="false" />
```
3. Change `port="8080"` to specify the desired port.
4. Stop and then restart the Tomcat service for the change to take effect.
5. Change the URL in all Entegra Browser shortcuts – for example, desktop and Start Menu shortcuts created by the Entegra install – to specify the correct port.

## Event Log Errors

The following error may occur in the Application Event Log on an Entegra machine:

```
The description for Event ID ( 1 ) in Source ( LMRepAgt )
cannot be found. The local computer may not have the necessary
registry information or message DLL files to display messages
from a remote computer. The following information is part of
the event: Repository server online: SERVER1
, C:\Memphis\Source\Audit\Repository\LMRepositoryAgent\CSrvObj.c
pp(564)
```

This error is not a program error but a problem causing Windows Event Viewer to display informational messages incorrectly. This problem generally means that you are viewing Entegra event log messages on a machine that does not have the necessary tools to interpret them. This problem can occur if you view the event log from a machine without Entegra components installed, or under certain circumstances if you have uninstalled Entegra.

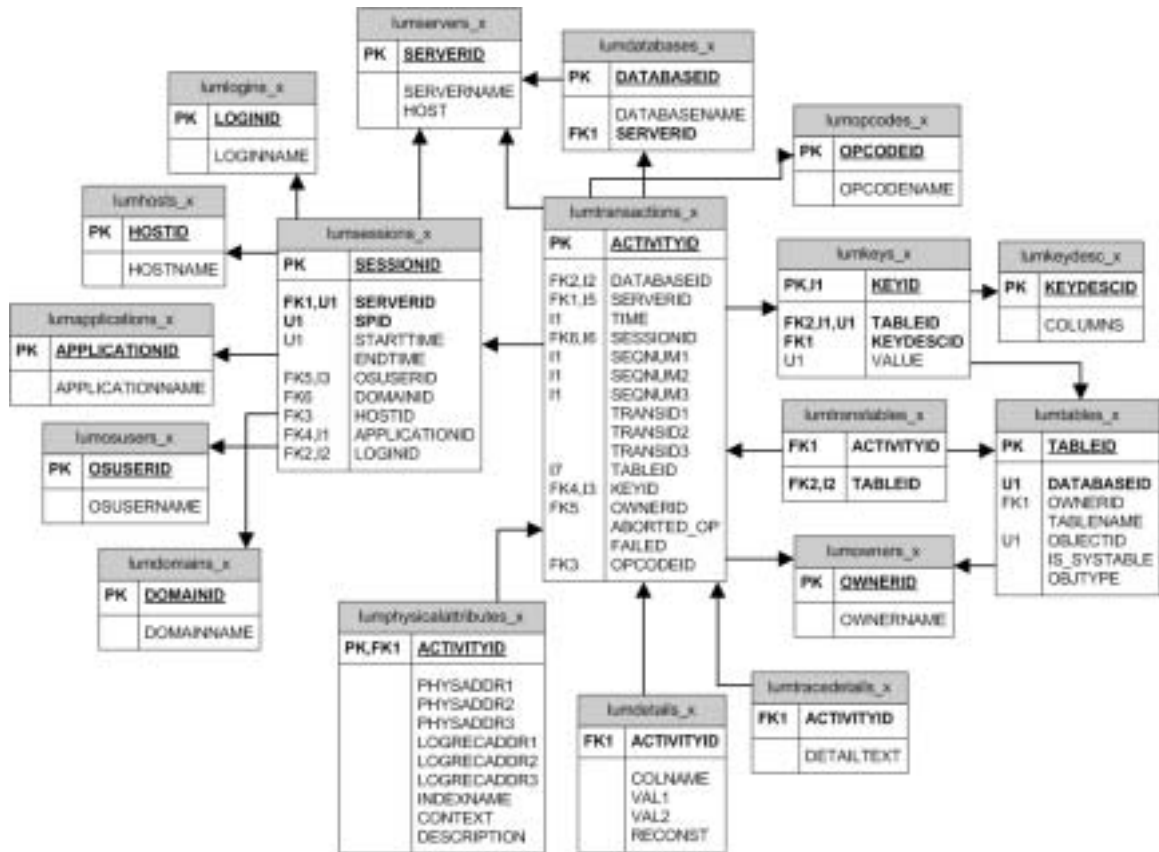
To work around this problem, view the Event Log from a computer that has Entegra components installed. Alternatively, you may ignore the initial text. The important part of the event is the text that appears after "The following information is part of the event."

# Appendix A: Repository Schema

This appendix provides an entity relationship diagram and tables for the schema structure of the Entegra Repository.

## Entity Relationship Diagram

The following diagram is the Entity Relationship Diagram for the Entegra Repository Schema.



# Schema Tables

The Repository schema is a normalized design that balances the requirements of the Entegra Browser, minimization of space used, and minimization of import time. The schema consists of eighteen tables.

Table	What it stores
lumtransactions_x	Stores audited activity data.
lumdetails_x	Stores details of each column change that occurred as a result of an audited transaction.
lumtracedetails_x	Stores details of each audited DDL or security event and SELECT text.
lumtables_x	Stores information about each audited table.
lumkeys_x	Stores the logical key for associated with modified row.
lumkeydesc_x	Stores the names of columns for each audited table that constitute a logical key.
lumservers_x	Stores information about each Audited Server.
lumdatabases_x	Stores information about each audited database.
lumsessions_x	Stores information about user logon sessions.
lumopcodes_x	Stores the names of opcodes.
lumtranstable_x	Links the lumtransactions_x table with the lumtables_x table to produce a one-to-many relationship.
lumowners_x	Stores the names of the SQL server object owners.
lumphysicalattributes_x	Stores low-level system information about each activity.
lumlogins_x	Stores login information.
lumosusers_x	Stored Windows login information.
lumapplications_x	Stores name of application used for session.
lumdomains_x	Stores domain name of client.
lumhosts_x	Stores name of host machine used for session.

In each table name, the "x" represents the name of the repository, as selected by the user when the repository is created. So if the repository is named Repos1, the tables are lumTransactions\_Repos1, lumDetails\_Repos1, etc.

The following sections provide more detail on the Repository tables.

## lumtransactions\_x

This is the main table that stores all audit data. There is one row in this table for each audited DML (insert/delete/update) transaction, each DDL transaction, each Security event, and SELECT statement.

activityid	numeric (18,0)	Unique ID for this row. This column is a foreign key with the lumdetails and lumtracedetails tables (see below).
keyid	numeric (18,0)	Foreign key to join against lumkeys table. This key is set for DML operations to identify the record which was changed by the operation.
sessionid	numeric (18,0)	Unique ID of the SQL login session during which the transaction occurred. Foreign key to lumsession table.
databaseid	int	Unique ID of the database on which the transaction occurred. Foreign key to lumdatabases table.
serverid	int	Unique ID of the audited server instance on which the transaction occurred. Foreign key to lumservers table.
time	datetime	Timestamp of the event.
transid1	int	High DWORD of system transaction ID for the event.
transid2	int	Middle DWORD of system transaction ID for the event.
transid3	int	Low DWORD of system transaction ID for the event.
seqnum1	int	High DWORD of unique sequence ID for the event. LSN for SQL Server, SCN for Oracle.
seqnum2	int	Middle DWORD of unique sequence ID.
seqnum3	int	Low DWORD of unique sequence ID.
opcodeid	int	Foreign key to lumOpCodes.
tableid	int	Obsolete. This field has been replaced by the lumtranstable_x table.
ownerid	int	Foreign key to lumOwners.
aborted_op	char(1)	Whether the event was part of an aborted transaction "1" if aborted, "0" otherwise.
failed	char(1)	Whether the event was part of a failed transaction "1" if failed, "0" otherwise.

## lumdetails\_x

This table stores column change details associated with INSERT, DELETE, and UPDATE operations. There is one row in this table for each change to a column – for example, a transaction that changed three columns would have three rows in this table (but only one row in the `lumtransactions` table). This table can be joined against `lumtransactions` through the `activityid` column to associate column changes with operations.

activityid	numeric (18,0)	An ID for the transaction; foreign key with <code>lumtransactions</code> .
colname	nvarchar (512)	Name of the column that was changed.
val1	ntext	New column value.
val2	ntext	Old column value.
reconst	char(1)	Reserved.

## lumtracedetails\_x

This table stores details associated with DDL and security events that were audited. There is one row in this table for each audited event. This table can be joined against `lumtransactions` through the `activityid` column to associate a transaction with the operations it performed.

activityid	numeric (18,0)	An ID for the transaction; foreign key with <code>lumtransactions</code> .
detailtext	ntext	String containing the details of the audited event. Typically, this is a SQL statement.



## lumtables\_x

This table stores a list of audited tables and views on the Audited Server, and can be joined with `lumtransactions` via the `lumtranstable` table.

tableid	int	A unique ID for this table or view.
databaseid	int	Unique ID for the database containing the table or view; foreign key with <code>lumdatabases</code> table.
tablename	nvarchar (256)	Name of the table or view.
objectid	nvarchar	The ID assigned to the table or view by the target server.
is_systable	char	Whether the table is a system table (1) or a user table (0).
objtype	int	Whether the object is a table (1) or a view (2).
ownerid	int	Foreign key to <code>lumOwners</code> .

## lumkeydesc\_x

This table stores the names of columns that make up the logical key for a table. This table may have at most one row for each audited table. The "columns" column here is a concatenation of the logical-key column names, delimited by semicolons.

keydescid	int	Foreign key with <code>lumkeys</code> .
columns	nvarchar (4000)	The column names that make the key.

## lumkeys\_x

This table stores key values associated with DML events in `lumtransactions`. Key column descriptions (column names that make the key) can be found by joining with `lumkeydesc`. The `value` column is a semicolon-delimited concatenation of all column values that make the key.

keyid	numeric (18,0)	Logical key, foreign key with <code>lumtransactions</code> .
tableid	int	Foreign key with <code>lumtables</code> .
keydescid	int	Foreign key with <code>lumkeydesc</code> .
value	nvarchar (4000)	Key value.

## Example of lumkeys and lumkeydesc\_x

The following shows a sample listing of contents of the lumkeys and lumkeydesc tables, to illustrate their purposes.

### lumkeydesc\_x:

keydescid	columns
1	employeeID
2	custID;lastname

### lumkeys\_x:

keyed	tableid	keydescid	value
1	1	1	5
2	2	2	12;Smith
3	2	2	13;Jones

In the example above, the audited table with tableID 1 uses the employeeID column as its logical key. The table with tableID 2 uses the custID and lastname columns as its logical key. For a unique row in table 1, the employeeID is 5. For a unique row in table 2, the custID is 12 and the lastname is Smith; for a second row in table 2, the custID is 13 and the lastname is Jones.

## lumservers\_x

This table stores information about audited server instances. Each audited server instance has one row in this table.

serverid	int	A unique ID for this audited server instance. This column is a logical key for this table and a foreign key with lumsession and lumdatabases.
servername	nvarchar (256)	Name of the server instance.
host	nvarchar (256)	Name of the machine on which the server instance is running.

## lumdatabases\_x

This table stores information about audited databases. Each audited database has one row in this table.

databaseid	int	A unique ID for this database. This column is a logical key for this table and a foreign key with lumtransactions and lumtables.
databasename	nvarchar (256)	Name of the database.
serverid	int	ID of the server instance that the database resides on; foreign key with lumservers.

## lumsessions\_x

This table stores information about user logon sessions on the audited server that resulted in audited transactions. Each session has one row in this table. You can join this table with lumtransactions to get a complete list of transactions performed by a particular session, or to get the session and user information for a particular transaction.

sessionid	numeric (18,0)	A unique ID for this session. This column is a logical key for this table and a foreign key with lumtransactions.
serverid	int	ID of the server on which the session occurred; foreign key with lumServers.
spid	int	System process ID to which the session was assigned.
starttime	datetime	Session start timestamp.
endtime	datetime	Session end timestamp.
osuserid	int	Foreign key with lumosusers.
domainid	int	Foreign key with lumdomains.
hostid	int	Foreign key with lumhosts.
applicationid	int	Foreign key with lumapplications.
loginid	int	Foreign key with lumlogins.

## lumphysicalattributes\_x

This table contains MSSQL server-specific physical attributes. This table stores low-level system information about the database activities. There is a one-to-one relationship between lumtransactions\_x and lumphysicalattributes\_x.

activityid	numeric (18,0)	Foreign key with lumtransactions.
physaddr1	int	High DWORD of physical row address. Physical row address of the row changed by the record. This address is set for DML log records.
physaddr2	int	Middle DWORD of physical row address.
physaddr3	int	Low DWORD of physical row address.
logrecaddr1	int	High DWORD of physical log record address.
logrecaddr2	int	Middle DWORD of physical log record address.
logrecaddr3	int	Low DWORD of physical log record address.
indexname	nvarchar (256)	Index name read from the log record.
context	nvarchar (256)	MSSQL internal log attribute text.
description	nvarchar (256)	

## lumhosts\_x

This table stores the names of the host machines used for the user logon sessions on the audited server.

hostid	int	Unique ID for the host, and a foreign key with lumsessions.
hostname	nvarchar (512)	Host machine name.

## lumdomains\_x

This table stores the names of the windows domain names for the user logon sessions on the audited server.

domainid	int	Unique ID for the domain, and a foreign key with lumsessions.
domainname	nvarchar (512)	Domain name.

## lumapplications\_x

This table stores the names of the applications used for the user logon sessions on the audited server.

applicationid	int	Unique ID for the application, and a foreign key with lumsessions.
applicationname	nvarchar (512)	Application name.

## lumlogins\_x

This table stores SQL server security login names for the user logon sessions that used SQL server authentication on the audited server.

loginid	int	Unique ID for the SQL server login, and a foreign key with lumsessions.
loginname	nvarchar (512)	Login name.

## lumosusers\_x

This table stores Windows username for user logon sessions that used NT Authentication to access the audited server.

osuserid	int	Unique ID for the user login, and a foreign key with lumsessions.
osusername	nvarchar (512)	OS user name.

## lumopcodes\_x

This table stores names of all auditable opcodes in Entegra.

opcodeid	int	Unique ID for the opcode, foreign key with lumtransactions
opcodename	nvarchar (512)	Op code name.

## lumtranstable\_x

This table joins the transactions table with the tables table. This table provides a one-to-many relationship between events (lumtransactions) and tables (lumtables).

activityid	numeric (18, 0)	Foreign key with lumtransactions.
tableid	int	Foreign key with lumtables.

## lumowners\_x

This table stores the names of the SQL server object owners.

ownerid	int	Unique ID for the object owner, and a foreign key with lumtransactions.
ownername	nvarchar (512)	Object owner/user name.

---

# Appendix B: Restrictions

This appendix lists the major restrictions for this version of Entegra.

## Component Setup Restrictions

The following restrictions apply to component setup.

- The Entegra Management Console cannot run on Windows NT 4.0 or earlier.
- A Repository Server Instance cannot run on SQL Server 7.0 or earlier. SQL Server 2000 is required.
- Collection Agents, Repository Agents, and Repositories cannot run on clustered servers.

## Auditing Restrictions

The following restrictions apply to auditing.

- ALTER DATABASE commands are currently not audited.
- Many alerts are not available for Audited Server Instances running SQL 7.0.
- Auditing of SELECTS does not work for SQL 7.0 (only SQL 2000).
- Entegra does not export updates to BLOB columns.

## Other Restrictions

Other restrictions include the following:

- The Entegra Browser does not accept Windows authentication for logging in to Repositories.
- The Import History view in the Entegra Management Console cannot be purged.





---

# Appendix C: Configuring the Entegra Web Server with IIS

This appendix provides the steps for configuring the Entegra Web Server with IIS.

## Procedure

This procedure is divided into two parts. Part 1 creates the virtual directory and Part 2 sets up the ISS web filter.

### Part 1. Create a new Virtual Directory

To create a new virtual directory, do the following:

1. Click *Start, Control Panel, Administrative Tools, Internet Information Server*.
2. Expand *Web Sites*, right-click *Default Web Site*, and then select *New, Virtual Directory*.  
The “Welcome to the Virtual Directory Creation” Wizard is displayed.
3. Click **Next**.  
The “Virtual Directory Alias” screen is displayed.
4. In the **Alias** text box, type **Lumigent Entegra**, and then click **Next**.  
The “Web Site Content Directory” screen is displayed.
5. In the Directory text box, type **C:\Program Files\Lumigent\Entegra\WebUI\server\bin**, and then click **Next**.  
The “Access Permissions” screen is displayed.
6. Select the **Read** and **Execute (such as ISAPI applications or CGI)** check boxes, clear the **Run Scripts (such as ASP)** check box, and then click **Next**.  
The “Finish” screen is displayed.
7. Click **Finish**.

### Part 2. Set up the IIS filter

To set up the IIS filter, do the following:

8. At the Navigation pane, right-click *Web Sites*, and then select **Properties**.  
The “Properties” screen is displayed.
9. At the **ISAPI Filters** tab, click **Add**.

The “Filter Properties” screen is displayed.

10. At the **Filter Name** text box, type **Entegra Redirect**.
  11. At the **Executable** text box, type or browse to **C: \Program Files\Lumigent\Entegra\WebUI \server\bin\i sapi \_redirect. dll**, and then click **OK**.
- The “Properties” screen is redisplayed.
12. Click **OK**.
  13. At the Services control panel, restart EntegraWebServer, and restart World Wide Web Publishing.
  14. Connect to **http: \machine-name\lumigent\login. html**

---

# Index

---

## A

- accessing the browser · 138
- add audited server instance wizard · 32
- add collection agent wizard · 35
- add database wizard · 33
- add repository server instance wizard · 34
- add repository wizard · 34
- add/remove columns
  - procedure · 57
- add/remove tables
  - procedure · 53
- add/remove tables wizard · 35
- add/remove views wizard · 35
- adding a collection agent
  - procedure · 60
- adding a database to audit
  - procedure · 50
- adding a repository
  - procedure · 48
- adding a repository server instance
  - procedure · 45
- adding a SQL server instance to audit
  - procedure · 36
- adding views
  - procedure · 59
- agent · *See* data collection agent
- architecture · *See* Entegra system architecture
- archive files · 9
- archiving
  - process · 119
- archiving options · 119
  - intermediate file handling · 121
  - purging the repository · 121
  - SQL backup log handling · 120
- audit data
  - purging · 122
  - restoring after purge · 124
- audit settings
  - individual tables · 54
  - multiple tables · 55
  - selecting
    - DELETE · 54
    - INSERT · 54
    - SELECT · 54

- UPDATE · 54
- audit status · 82
- audited objects · 4
- audited server-level options · 129

---

## B

- browser
  - columns
    - showing/hiding · 140
    - sorting · 140
  - columns displayed · 140
  - filtering data · 141
  - log on · 138
  - navigation pane · 139
  - permissions · 137
  - viewing · 139
  - viewing details · 141

---

## C

- change collection agent wizard · 35
- changing a collection agent
  - procedure · 64
- collection agent · *See* data collection agent
- collection history · 129
  - purging · 130
- configuration · 31
  - examples · 67
  - optional tasks · 31
  - required tasks · 31
  - setting up three machines example · 82
  - setting up two machines example · 68
- wizards
  - add audited server instance · 32
  - add collection agent · 35
  - add database · 33
  - add repository · 34
  - add repository server instance · 34
  - add/remove tables · 35
  - add/remove views · 35
  - change collection agent · 35
  - overview · 32
- configuring the web server with IIS · 159
- custom reports · 9

---

## D

data  
    types of data collected · 6  
data collection agent · 4, 134  
    agent-level options · 135  
    definition · 6  
    process · 6  
database  
    permissions · 137  
database-level options · 130  
DELETE  
    selecting · 54

---

## E

EMC · *See* Entegra Management Console  
Entegra  
    browser  
        viewing · 139  
    capabilities · 1  
    components · 3  
    configuration · 5  
        optional tasks · 6  
        required tasks · 5  
    configuring the web server with IIS · 159  
    functions · 5  
    management console-level options · 128  
    restrictions · 157  
    system architecture · 3  
    web browser · 5  
    web server · 5  
Entegra Management Console · 5  
    description · 31  
Entegra software  
    registering · ii  
    technical support · ii  
event log errors · 145

---

## F

first installation · *See* initial Entegra installation

---

## I

IIS  
    configuring the Entegra Web Server · 159  
import history folder · 133  
improving performance · 32, 142  
Information resources  
    FAQ · i  
    online Help · i  
    User Manual · i  
initial Entegra installation · 36  
INSERT  
    selecting · 54  
installation

    audited server instance requirements · 12  
    collection agent requirements · 13  
    EMC requirements · 13  
    Entegra browser requirements · 13  
    initial Entegra  
        overview · 36  
    network requirements · 13  
    overview · 11  
    prerequisites · 17  
    procedure · 17  
    repository agent requirements · 12  
    repository server requirements · 12  
    requirements · 12  
    security requirements · 13  
    web server requirements · 12  
interactive reports · 9

---

## L

license key  
    described · 81  
    SELECT · 28  
LMRestore command · 122  
    example · 126  
logical keys · 7  
    default setting · 7  
lumapplications\_x table · 155  
lumdatabases\_x table · 153  
lumdetails\_x table · 150  
lumdomains\_x table · 154  
lumhosts\_x table · 154  
Lumigent Technologies  
    contacting · ii  
    email · ii  
    web site · ii  
lumkeydesc\_x table · 151  
    example · 152  
lumkeys\_x table · 151  
    example · 152  
lumlogins\_x table · 155  
lumopcodes\_x table · 155  
lumosusers\_x table · 155  
lumowners\_x table · 156  
lumphysicalattributes\_x table · 154  
lumservers\_x table · 152  
lumsessions\_x table · 153  
lumtables\_x table · 151  
lumtracedetails\_x table · 150  
lumtransactions\_x table · 149  
lumtranstable\_x table · 156

---

## P

permissions  
    on lumigent database · 137  
    on repository database · 137  
procedure  
    accessing the browser · 138  
    add/remove columns · 57

- add/remove tables · 53
- adding a collection agent · 60
- adding a database to audit · 50
- adding a repository · 48
- adding a repository server instance · 45
- adding a SQL server instance to audit · 36
- adding views · 59
- changing a collection agent · 64
- configuring the web server with IIS · 159
- installing Entegra · 17
- purging the repository · 122
- removing views · 59
- restoring purged audit data · 124
- selecting the logical key · 58
- upgrading the EMC · 20
- upgrading the Web Server · 25
- purging
  - collection history · 130
  - repository data · 9, 121

---

## R

- removing views
  - procedure · 59
- reports
  - custom · 9
  - interactive · 9
  - scheduled · 9
- repository · 7
  - definition · 4
  - disk space required · 12
  - permissions · 137
  - purging audit data · 122
  - restoring purged data · 124
  - schema
    - entity relationship diagram · 147
    - table structure · 148
  - server-level options · 133
- repository agent · 4
  - definition · 7
- repository schema · 147
- repository-level options · 134
- restoring
  - archived data · 122
  - purged audit data procedure · 124
- restrictions
  - component setup · 157

---

## S

- scheduled reports · 9
- schema table
  - lumapplications\_x · 155
  - lumdatabases\_x · 153
  - lumdetails\_x · 150
  - lumdomains\_x · 154
  - lumhosts\_x · 154
  - lumkeydesc\_x · 151
  - lumkeys\_x · 151

- lumlogins\_x · 155
- lumopcodes\_x · 155
- lumosusers\_x · 155
- lumowners\_x · 156
- lumphysicalattributes\_x · 154
- lumservers\_x · 152
- lumsessions\_x · 153
- lumtables\_x · 151
- lumtracedetails\_x · 150
- lumtransactions\_x · 149
- lumtranstable\_x · 156
- schema tables · 148
- security requirements · 13
  - audited server machine · 14
  - collection agent machine · 16
  - repository · 16
  - repository machine · 16
- SELECT
  - adding
    - overview · 28
    - prerequisites · 28
    - procedure · 28
  - auditing · 7
  - license key · 28
  - selecting · 54
- selecting the logical key
  - procedure · 58
- service login privileges · 14
- status history · 82
- storing data · *See* repository

---

## T

- table-level options · 132
- technical support · ii
- troubleshooting · 143

---

## U

- UPDATE
  - selecting · 54
- upgrading the EMC · 20
  - prerequisites · 20
  - procedure · 20
- upgrading the Web Server
  - procedure · 25
- using multiple Entegra Management Consoles · 67
  - caution · 67

---

## W

- wizards
  - add audited server instance · 32
  - add collection agent · 35
  - add database · 33
  - add repository · 34
  - add repository server instance · 34
  - add/remove tables · 35

add/remove views · 35

change collection agent · 35